Security and Emergency Operations

Executive Budget Summary

Mission

Provide domestic Nuclear Safeguards and Security for the protection of nuclear weapons, nuclear materials, nuclear facilities, and classified and unclassified information; against theft, sabotage, espionage, terrorist activities, or any loss or unauthorized disclosure that could endanger our National Security or disrupt operations. *Cyber Security* provides policy, planning, and technical development, to ensure consistent standards and requirements are implemented for the protection of classified and unclassified information used or stored on Departmental systems. *Foreign Visits and Assignments* provides a centralized focus to track and analyze the details of all foreign visits and assignments for all DOE facilities to ensure that these visits and assignments are conducted in a secure manner. *Physical Security* provides cost-effective plans, policies, and technical solutions required to protect the Department's critical assets with an R&D emphasis on nuclear, biological, and chemical weapons protection and detection equipment and training. *Plutonium, Uranium, and Special Materials Inventory* maintains real-time, reliable, and complete information on DOE nuclear materials that are subject to special control and accounting procedures. *Critical Infrastructure Protection* ensures the viability of the energy sector infrastructure nationwide. *Classification/Declassification* provides the appropriate level of classification of information to help ensure its protection with an emphasis on declassification of previously classified documents for greater public access.

Conduct Security Investigations in the form of background investigations to provide appropriate security clearances. This ensures that DOE Federal and contractor personnel who, in the performance of their official duties, have the appropriate level of authorizations for Restricted Data, National Security Information, or special nuclear materials.

Provide a Corporate Management Information Program (CMIP), which is the Department's corporate investment initiative to replace outdated corporate information systems. CMIP provides a managed, disciplined, and cost-effective way to modernize DOE corporate business systems in a coordinated manner which uses new and emerging technologies and practices under the direction of the Department's Chief Information Officer.

Support Program Direction for all Federal personnel and other contractual support required at DOE Headquarters, and one field office to carry out the program's mission in a cost effective and efficient manner. The budget request specifically reflects the support of the Chief Information Officer, Security Affairs, Critical Infrastructure Protection, Resource Management, and the Office of the Director.

Program Overview

The Office of Security and Emergency Operations (SO) is charged with developing the policies that govern the protection of national security and other assets entrusted to the Department of Energy. SO also provides safeguards and security training and field assistance to Departmental facilities to ensure the ability to efficiently and effectively implement Departmental policy. The Department established the Office of Security and Emergency Operations to work with the Secretary of Energy to implement a comprehensive plan that gives DOE the tools and authority to correct institutional problems and protect America's nuclear secrets. *This program supports the National Nuclear Security General Goal in the Department's September 2000 Strategic Plan:* **Enhance national security through military application of nuclear technology and reduce the global danger from weapons of mass destruction.**

Program History

In past decades, safeguards and security (S&S) within DOE, and its predecessor organizations functioned with abundant resources, featuring uncompromising risk-avoidance, in-depth and layered defense, and redundant security services. The program was well-funded and labor intensive, with strong administrative controls. In the early 1990's with the end of the Cold War and advent of major arms reduction agreements, DOE realigned its priorities. The contemplated future weapons complex would be potentially smaller, less diverse, and less expensive to operate. A critical element of this "downsizing" was to be the maximum consolidation of special nuclear material (SNM) at the minimum number of secure locations. The Department's redirected national security mission concentrated on nonproliferation, safe dismantlement of nuclear weapons and secure maintenance of the stockpile in the absence of underground nuclear testing. Accordingly, the DOE S&S program changed significantly, but it did not keep pace with other dynamic developments in the direction of the rest of the Department.

Over the years, the Department's focus on security became diminished. There was no one office accountable for DOE critical security requirements, and individual accountability decreased. This organizational lack of focus led to a deterioration of security awareness and education. Employees and contractors were not continually made aware of their personal security responsibilities. Cyber security practices were not keeping pace with the threats posed by increased computer hacking and cyber terrorism; and there was a gradual erosion of resources required to improve cyber capabilities. Cases of inadequate protection practices were highlighted in more than 20 security reports, studies, and evaluations during the last decade. The Secretary directed an abrupt end to this unacceptable situation.

In May 1999, a Security Reform Package proposed the most sweeping reform of security programs in the Department's history. This comprehensive plan involved the creation of the Office of Security and Emergency Operations (SO), the enhancement of the Office of Counterintelligence, and the elevation and revitalization of the Office of Independent Oversight and Performance Assurance.

The SO Office was established in July 1999, and incorporated a single cyber security organization under the direction of the Chief Information Officer. A new Office of Plutonium, Uranium, and Special Materials Inventory was established with responsibility for maintaining real-time, reliable and complete information on DOE nuclear materials subject to special control and accounting procedures. This Office serves as the Department's primary source for reliable inventory information on those DOE nuclear materials. An Office of Foreign Visits and Assignments was formed to centralize tracking and analysis of all foreign visits and assignments for all DOE facilities to ensure that these are conducted in a secure manner. A new Office of Critical Infrastructure Protection was also established in October 1999 to address energy infrastructure security requirements.

Objective

Ensure that the Department's nuclear weapons, materials, facilities, and information assets are secure through effective safeguards and security policy, implementation, and oversight.

Performance Goals

Goal 1: Prevent the theft, loss or unauthorized use of nuclear weapons, nuclear weapon components, special nuclear materials as well as classified and unclassified information and assets.

Goal 2: Reduce DOE site vulnerability and risk and national energy emergency vulnerabilities.

Goal 3: Direct fund DOE safeguards and security costs to facilitate improvements in planning, management, direction, tracking, and monitoring of the safeguards and security program.

Strategies

\# **Goal 1, Strategy 1** Develop and implement cost-effective plans, policies, and technical solutions required to protect the Department's critical assets; which include nuclear weapons in DOE custody, nuclear weapons components, special nuclear materials, classified information and DOE facilities against a spectrum of threats, including terrorist activity, sabotage, espionage, theft, diversion, loss or unauthorized use.

\# **Goal 1, Strategy 2** Maintain inventory control of plutonium (Pu) and Highly Enriched Uranium (HEU).

\# **Goal 1, Strategy 3** Effectively maintain information on visits and assignments by foreign nationals to DOE Federal and contractor sites.

\#   **Goal 1, Strategy 4** Audit documents declassified by DOE and other agencies to ensure that nuclear weapon design information is not inadvertently released, and review DOE information to classify that which warrants protection in the interest of national security and declassify that which does not warrant such protection.

\#   **Goal 1, Strategy 5** Continuously oversee and measure the effectiveness of on-going S&S programs and their ability to prevent unacceptable threats from occurring.

\#   **Goal 1, Strategy 6** Provide domestic technology and systems development to ensure the availability of state-of-the-art technical capabilities for accountability and control of nuclear material; storage of special nuclear materials; protection of sensitive DOE facilities and national security interests, including classified matter.

\#   **Goal 1, Strategy 7** Protect DOE nuclear facilities, employees and the environment by providing a counter terrorist capability to detect and assess adversarial use of nuclear, chemical, or biological weapons of mass destruction.

\#   **Goal 1, Strategy 8** Develop and implement a comprehensive cyber security program that implements risk-based policies; provides comprehensive cyber security education, awareness, and training; implements capabilities at all sites for cyber incident response, baseline architecture, cyber intrusion detection and reporting, and public key architecture; and provides tools to eliminate cyber security vulnerabilities.

\#   **Goal 1, Strategy 9** Maintain personnel security and security investigations programs to meet the Department's requirements for cleared personnel who require access authorizations for Restricted Data, National Security Information, or special nuclear materials.

\#   **Goal 2, Strategy 1** Work with energy infrastructure stakeholders to design and develop technical methodologies to enhance the protection of critical infrastructure assets.

\#   **Goal 2, Strategy 2** Reduce DOE facilities' vulnerability to chemical and biological threats through sensor and protective equipment evaluations.

\#   **Goal 2, Strategy 3** Conduct education and training programs that will ensure up-to-date training of protective force personnel and technical S&S staff.

\#   **Goal 3, Strategy 1** Strengthen the ability to manage S&S as an activity with a specifically identified budget and the ability to enhance awareness of S&S issues throughout the National Nuclear Security Administration and the DOE complex.

Performance Measures

\#   **Goal 1, Strategy 1, Performance Measure 1** Modernize the information security program to analyze and deter major incidents involving the compromise of classified information.

\#   **Goal 1, Strategy 1, Performance Measure 2**   Support the establishment of an Integrated Safeguards and Security Management program through issuance of policy and guidelines.

\#   **Goal 1, Strategy 1, Performance Measure 3**   Enhance the Department's protective force capabilities to meet the current and future spectrum of threats.

\#   **Goal 1, Strategy 1, Performance Measure 4**   Address enhanced protection measures for the most critical nuclear weapon design information and test the effectiveness of protective forces and S&S systems on a recurring basis.

\#   **Goal 1, Strategy 1, Performance Measure 5**   Implement a revised DOE protective force order which addresses planning, training, and exercises to prepare for a weapon of mass destruction event.

\#   **Goal 1, Strategy 2, Performance Measure 1**   Maintain baseline measurement uncertainty information on Pu and HEU inventories and identify where accountability information is inadequate.

\#   **Goal 1, Strategy 2, Performance Measure 2**   Upgrade the Nuclear Materials Management and Safeguards System.

\#   **Goal 1, Strategy 3, Performance Measure 1**   Provide an effective system for tracking and managing foreign visits at DOE facilities that supports rapidly changing and growing national security needs.

\#   **Goal 1, Strategy 4, Performance Measure 1**   Continue the classification guidance streamlining initiative, issuing additional guides in the streamlined format.

\#   **Goal 1, Strategy 5, Performance Measure 1**   Identify the need for S&S enhancements through the use of on-site evaluations and review of site S&S plans.

\#   **Goal 1, Strategy 6, Performance Measure 1**   Modify current or develop new technologies for S&S applications to reduce the backlog of documented and validated field user needs by about 40%.

\#   **Goal 1, Strategy 7, Performance Measure 1**   Review the development and implementation of countermeasures designed to mitigate the effectiveness of nuclear, biological, and chemical weapons of mass destruction events.

\#   **Goal 1, Strategy 8, Performance Measure 1**   Implement the Cyber Security Program Action Plan.

\#   **Goal 1, Strategy 8, Performance Measure 2**   Implement cyber security architecture upgrades across the DOE complex.

\#   **Goal 1, Strategy 8, Performance Measure 3**   Provide cyber security education, training, and awareness for individuals responsible for implementing cyber security and protective measures.

\#   **Goal 1, Strategy 8, Performance Measure 4**   Maintain a centralized incident response capability to provide incident analysis of cyber intrusions and attempted intrusions, and warning capability for all DOE sites.

Ensure the timely and efficient processing of

- # **Goal 1, Strategy 9, Performance Measure 1** Ensure the timely and efficient processing of approximately 25,000 personnel security investigations needed for initial access authorizations and reinvestigations for the DOE complex.

- # **Goal 1, Strategy 9, Performance Measure 2** Review the types and numbers of investigations to ensure consistency with DOE mission changes, considering heightened security requirements.

- # **Goal 1, Strategy 9, Performance Measure 3** Ensure that the quality of an investigative product is sufficient for DOE security needs.

- # **Goal 2, Strategy 1, Performance Measure 1** Work with the national energy sector toward developing the capability for assuring the nation's energy infrastructures, including identifying the physical and cyber vulnerabilities and interdependencies of the electric power, oil, and gas infrastructures.

- # **Goal 2, Strategy 1, Performance Measure 2** Develop and identify DOE technologies and approaches that can help assure our nation's critical energy infrastructures and facilitate their use by the private sector and other Federal agencies.

- # **Goal 2, Strategy 2, Performance Measure 1** Demonstrate improved counter-terrorism response capability to the use of Weapons of Mass Destruction through interagency exercises and training.

- # **Goal 2, Strategy 3, Performance Measure 1** Conduct 175 S&S training courses at the Nonproliferation and National Security Institute with approximately 200 iterations.

- # **Goal 3, Strategy 1, Performance Measure 1** Annually review the efficiency of S&S resources.

Significant Accomplishments and Program Shifts

- # Issuance of a "Zero Tolerance" policy with regard to security violations. This policy provides clear guidance on personal accountability for protecting classified and other sensitive materials and ensures accountability of performance in DOE's management contracts of its field sites.

- # Developed 42 new policies covering security over the past year to include the timely reporting of security incidents. An additional 35 are in various stages of concurrence and will be forthcoming soon.

- # Instituted numerous cyber-security enhancements addressing issues such as warning banners, password generation, protection and use, control of access to DOE automated information systems by foreign nationals.

- # Mounted an aggressive and comprehensive security education and awareness campaign to remind each and every individual of their security obligations. These obligations were further reinforced through a series of complex-wide security stand-downs.

- # Greatly improved operations in numerous areas ranging from the way we train our security personnel to the way we validate our field site security plans.

\# In FY 2001, funding for field non-federal employees security investigations, excluding those from the Office of Naval Reactors, will be directly funded in the Security Investigations budget rather than from the program office budgets, for the first time since FY 1998.

\# Implemented regional infrastructure assurance activities to assist energy industry and state and local government to prepare for and respond to disruptions.

\# A new decision unit has been created to provide funding for the Corporate Management Information Program (CMIP). CMIP is the Department's corporate investment initiative to replace outdated corporate information systems. CMIP provides a managed, disciplined, and cost-effective way to modernize DOE corporate business systems in a coordinated manner which uses new and emerging technologies and practices under the direction of the Department's Chief Information Officer. This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.

\# Program Direction now supports the desktop information technology requirements provided through the Chief Information Officer for Local Area Network connectivity, e-mail services, hardware and software acquisitions, and networking upgrades. This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.

\# The Office of Emergency Operations and its associated Program Direction within the Other Defense Activities appropriation has recently been transferred. Crosswalk tables of all funding for FY 2002 as well as comparable funding amounts for FY 2000 and FY 2001 are included in the comparability matrices at the end of this Executive Summary.

  ! The HAZMAT Spill Test Facility at the Nevada Test Site has been transferred from Emergency Management in the Other Defense Activities appropriation to the Nonproliferation and Verification Research and Development decision unit in the Defense Nuclear Nonproliferation appropriation for the National Nuclear Security Administration (NNSA).

  ! The Program Direction associated with the HAZMAT Spill Test Facility has been transferred from SO Program Direction in the Other Defense Activities appropriation to the Program Direction decision unit in the Defense Nuclear Nonproliferation appropriation for the National Nuclear Security Administration (NNSA).

  ! The Program Direction associated with the energy emergencies responsibilities of Emergency Management have been transferred to the Office of Critical Infrastructure Protection and remain in the SO Program Direction budget.

  ! The remainder of Emergency Operations, including all Emergency Response assets as well as Emergency Management have been transferred to the Readiness in Technical Base and Facilities decision unit under the Weapons Incident Response program in the Weapons Activities appropriation for the National Nuclear Security Administration.

!   The remainder of Program Direction associated with Emergency Operations has been transferred to the Program Direction decision unit in the Weapons Activities appropriation for the National Nuclear Security Administration.

Major Issues

\#   The Office of Security and Emergency Operations (SO) plans to operate at a program level significantly above FY 2001 new budget authority using FY 2000 unobligated balances carried over in to this fiscal year. While these carryover balances avoid major shortfalls in FY 2001, the potential exists for shortfalls in future years as security requirements are implemented. Although new budget authority for Security Investigations and, to a lesser extent, Nuclear Safeguards and Security appear to be significantly increasing in FY 2002; the program levels being executed in FY 2001 are higher. Also, after new requirements in FY 2002 for desktop information technology and work for others are removed, the Program Direction budget supports a lower program level than in FY 2001.

\#   SO has responsibility for developing the policies that govern the protection of national security and other assets entrusted to the DOE and direct responsibility for the security and information operations for the DOE Headquarters complex. Based on Congressional action in FY 2001, as well as the Department's revised security mission, SO has the responsibility to ensure that safeguards and security (S&S) policies are adequately supported by program offices. Accordingly, SO has a leading role in the Corporate Budget Reviews chaired by the Deputy Secretary in which the Department's S&S policy and resource recommendations are reviewed and initial budget decisions are made. In this capacity, SO is a key participant in S&S budget formulation, by coordinating with all programs to determine the sufficiency of resources and assisting in preparing adequate justifications for approved policies. Implementation of policy and execution of S&S budgets for DOE field activities is the responsibility of the Principal Secretarial Officers who are the line managers of the Department's program sites. However, SO does retain a role in reviewing and conferring with the program offices to ensure that stated S&S objectives are achieved. As such, SO is also responsible for approving necessary S&S funding adjustments and coordinating related budget amendments or reprogramming actions.

_____

Joseph S. Mahaley, Acting Director
Office of Security and Emergency Operations

8-30-01
_____
Date

Security and Emergency Operations Decision Unit Summary

(dollars in thousands)

	FY 2000	FY 2001	FY 2002	$ Change	% Change
Other Defense Activities					
Nuclear Safeguards and Security					
S&S Operational Support/Technology Dev.	59,083	63,133	67,133	4,000	6.3%
Cyber Security	17,318	30,243	30,243	0	0.0%
Critical Infrastructure Protection	2,100	2,994	2,994	0	0.0%
Classification/Declassification	17,067	20,818	20,818	0	0.0%
Subtotal, Nuclear Safeguards and Security .	95,568	117,188	121,188	4,000	3.4%
Security Investigations	37,577	32,927	44,927	12,000	36.4%
Corporate Management Information Program	0	0	20,000	20,000	100.0%
Program Direction	82,919	80,422	83,135	2,713	3.4%
Subtotal, Other Defense Activities	216,064	230,537	269,250	38,713	16.8%
Comparability for S&S general reduction . .	-878	0	0	0	0.0%
Security charge against reimbursable work	0	0	-712	-712	n/a
Offset to user organizations	-4,913	0	0	0	0.0%
Total, Other Defense Activities	210,273	230,537	268,538	38,001	16.5%

Security and Emergency Operations Site Funding Estimates

	FY 2000	FY 2001	FY 2002	$ Change	% Change
			(dollars in thousands)		
Other Defense Activities					
Albuquerque Operations Office	35,848	40,059	47,023	6,964	17.4%
Chicago Operations Office	7,699	8,026	8,916	890	11.1%
Idaho Operations Office	1,682	2,377	1,974	-403	-17.0%
Nevada Operations Office	2,273	2,346	3,577	1,231	52.5%
Oak Ridge Operations Office	8,633	7,852	7,497	-355	-4.5%
Oakland Operations Office	15,856	16,915	22,935	6,020	35.6%
Ohio Field Office	100	140	100	-40	-28.6%
Pittsburgh Naval Reactors Office	1,795	0	0	0	0.0%
Richland Operations Office	6,492	7,092	5,427	-1,665	-23.5%
Rocky Flats Area Office	0	140	0	-140	-100.0%
Savannah River Operations Office	4,222	5,824	6,152	328	5.6%
Schenectady Naval Reactors Office	660	0	0	0	0.0%
Washington Headquarters	130,804	139,766	165,649	25,883	18.5%
Subtotal, Other Defense Activities	216,064	230,537	269,250	38,713	16.8%
Comparability for S&S general reduction . .	-878	0	0	0	0.0%
Security charge against reimbursable work	0	0	-712	-712	n/a
Offset to user organizations	-4,913	0	0	0	0.0%
Total, Other Defense Activities	210,273	230,537	268,538	38,001	16.5%

Federal Staffing Estimates

	FY 2000	FY 2001	FY 2002
		(whole FTEs)	
Other Defense Activities			
Chicago Operations Office FTEs	56	58	58
Headquarters FTEs	278	329	329
Total, Full Time Equivalents	334	387	387

FY 2000 Comparability Matrix

New Structure

	Other Defense Activities	Defense Nuclear Nonproliferation		Weapons Activities		
	Nuclear S&S	Nonprolif.&Verif. R&D	Program Direction	RTBF	Program Direction	**Totals**
Old Structure						
Other Defense Activities						
Emergency Management						
Operations	-	-	-	13,282	-	13,282
HAZMAT facility	-	1,500	-	-	-	1,500
Comm. Center/Special Facility	1,143	-	-	-	-	1,143
	1,143	1,500	-	13,282	-	15,925
Emergency Response						
Assets other than NEST/ARG	-	-	-	-	-	-
	-	-	-	-	-	-
Program Direction	-	-	111	-	6,860	6,971
	-	-	111	-	6,860	6,971
Weapons Activities						
Emergency Response						
NEST/ARG	-	-	-	57,049	-	57,049
Assets other than NEST/ARG	-	-	-	14,691	-	14,691
	-	-	-	71,740	-	71,740
Program Direction					2,192	2,192
Totals	1,143	1,500	111	85,022	9,052	96,828

FY 2001 Comparability Matrix

New Structure

	Other Defense Activities	Defense Nuclear Nonproliferation		Weapons Activities		
	Nuclear S&S	Nonprolif.&Verif. R&D	Program Direction	RTBF	Program Direction	**Totals**
Old Structure						
Other Defense Activities						
Emergency Management						
Operations	-	-	-	11,576	-	11,576
HAZMAT facility	-	1,500	-	-	-	1,500
Comm. Center/Special Facility	1,143	-	-	-	-	1,143
	1,143	1,500	-	11,576	-	14,219
Emergency Response						
Assets other than NEST/ARG	-	-	-	19,183	-	19,183
	-	-	-	19,183	-	19,183
Program Direction	-	-	111	-	12,230	12,341
	-	-	111	-	12,230	12,341
Weapons Activities						
Emergency Response						
NEST/ARG	-	-	-	55,039	-	55,039
Assets other than NEST/ARG	-	-	-	-	-	-
	-	-	-	55,039	-	55,039
Program Direction	-	-	-	-	-	-
Totals	1,143	1,500	111	85,798	12,230	100,782

Department of Energy
FY 2002 Congressional Budget Request
Emergency Operations
(dollars in thousands)

FY 2002 Comparability Matrix

New Structure

| | Other Defense Activities | Defense Nuclear Nonproliferation | | Weapons Activities | | |
	Nuclear S&S	Nonprolif.&Verif. R&D	Program Direction	RTBF	Program Direction	**Totals**
Old Structure						
Other Defense Activities						
Emergency Management						
Operations	-	-	-	12,952	-	12,952
HAZMAT facility	-	1,500	-	-	-	1,500
Comm. Center/Special Facility	1,143	-	-	-	-	1,143
	1,143	1,500	-	12,952	-	15,595
Emergency Response						
Assets other than NEST/ARG	-	-	-	20,903	-	20,903
	-	-	-	20,903	-	20,903
Program Direction	-	-	111	-	12,230	12,341
	-	-	111	-	12,230	12,341
Weapons Activities						
Emergency Response						
NEST/ARG	-	-	-	55,270	-	55,270
Assets other than NEST/ARG	-	-	-	-	-	-
	-	-	-	55,270	-	55,270
Program Direction	-	-	-	-	-	-
Totals	1,143	1,500	111	89,125	12,230	104,109

Nuclear Safeguards and Security

Program Mission

The Nuclear Safeguards and Security Program provides effective policy, programmatic direction and training for the protection of the Department of Energy's (DOE) nuclear weapons, nuclear materials, classified information, and facilities. The program provides technology development and technical support to domestic safeguards and security activities as well as implementation of effective classified information and information control policies, accounting and control of nuclear material in the U.S. Government, and the development of policy for and protection of cyber assets. The program will help ensure protection of the energy infrastructure against both physical and cyber attacks. This program supports the National Nuclear Security objective in the Department's September 2000 Strategic Plan which ensures that the Department's nuclear weapons, materials, facilities, and information assets are secure through effective safeguards and security policy, implementation, and oversight.

Program Goal

Prevent the theft, loss, or unauthorized use of nuclear weapons, nuclear weapon components, special nuclear materials as well as classified and unclassified information and assets. Reduce DOE site vulnerability and risk and national energy emergency vulnerabilities.

Program Objectives

Develop and implement cost-effective plans, policies, and technical solutions required to protect the Department's critical assets; which include nuclear weapons in DOE custody, nuclear weapons components, special nuclear materials, classified information and DOE facilities against a spectrum of threats, including terrorist activity, sabotage, espionage, theft, diversion, loss or unauthorized use.

Maintain inventory control of plutonium (Pu) and Highly Enriched Uranium (HEU).

Effectively maintain information on visits and assignments by foreign nationals to DOE Federal and contractor sites.

Audit documents declassified by DOE and other agencies to ensure that nuclear weapon design information is not inadvertently released, and review DOE information to classify that which warrants protection in the interest of national security and declassify that which does not warrant such protection.

Continuously oversee and measure the effectiveness of on-going S&S programs and their ability to prevent unacceptable threats from occurring.

Provide domestic technology and systems development to ensure the availability of state-of-the-art technical capabilities for accountability and control of nuclear material; storage of special nuclear materials; protection of sensitive DOE facilities and national security interests, including classified matter.

Protect DOE nuclear facilities, employees and the environment by providing a counterterrorist capability to detect and assess adversarial use of nuclear, chemical, or biological weapons of mass destruction.

Develop and implement a comprehensive cyber security program that implements risk-based policies; provides comprehensive cyber security education, awareness, and training; implements capabilities at all sites for cyber incident response, baseline architecture, cyber intrusion detection and reporting, and public key architecture; and provides tools to eliminate cyber security vulnerabilities.

Maintain personnel security program to meet the Department's requirements for cleared personnel who require access authorizations for Restricted Data, National Security Information, or special nuclear materials.

Work with energy infrastructure stakeholders to design and develop technical methodologies to enhance the protection of critical infrastructure assets.

Reduce DOE facilities' vulnerability to chemical and biological threats through sensor and protective equipment evaluations.

Conduct education and training programs that will ensure up-to-date training of protective force personnel and technical S&S staff.

Significant Accomplishments and Program Shifts

In FY 2000, funding for the Nuclear Safeguards and Security program was appropriated in the Nonproliferation and National Security budget. As a result of the DOE-wide security reform announced on May 11, 1999, the Nuclear Safeguards and Security program was transferred to the Office of Security and Emergency Operations. Beginning with FY 2001, funding for this program will be budgeted for in the Office of Security and Emergency Operations budget request.

The Nuclear Materials Management and Safeguards System (NMMSS) was transferred from the Office of Arms Control and Nonproliferation to the Office of Security Affairs. In FY 2000, this program was appropriated in the Arms Control budget. However, for comparability purposes, FY 2000 funding for this activity is reflected in this budget request.

FY 2000 marked the first full year of operations for the re-established Unclassified Foreign Visits & Assignments Program; in June 2000, the Foreign Access Central Tracking System (FACTS), a web based system with automated routing, on line documentation, and transparent audit capability, went operational to support the vetting and approval policies for foreign national visitors and assignees issued by the Secretary

on July 14, 1999. Going into FY 2001, program staff initiated training, developed program policy, managed the Congressional moratorium on local approvals for foreign nationals from sensitive countries to visit or be assigned to the weapons labs (all such approvals were done personally by the Secretary during the moratorium), accepted policy and program responsibility for Classified Foreign Visits, Unofficial Foreign Travel, initiated a partnership with the Office of the Chief Financial Officer to support implementation of Official Foreign Travel, and initiated contact and consultation liaison with other Federal agencies managing similar responsibilities for foreign visitor/assignee programs.

\# The development of advanced safeguards and security technologies have resulted in millions of dollars in savings and cost avoidance for the Department. The following are some examples of technologies that are planned to be implemented around the DOE complex: a security sensor and biometric alarm multiplexing and communications system which allows DOE sites to transmit large numbers of alarms between sensors and command centers; significant improvements in the standard DOE vulnerability assessment tool (ASSESS) to incorporate several new capabilities as requested by DOE site vulnerability assessment teams; security system design manuals; the multi-platform trusted copy product to provide an authorized method to transfer unclassified text files from classified to unclassified IBM compatible personal computers; spent fuel measurement systems to two sites enabling them to safely measure and account for foreign and domestic special nuclear materials previously unmeasurable in the fuel; small nuclear detectors and multichannel analyzers to enable DOE facilities to measure and account for significant "hold up" quantities of nuclear materials in miles of piping; software enhancements to enable fielded nuclear materials accountability systems to measure previously unmeasurable isotopes of uranium, plutonium, neptunium and americium; multi-site operational evaluations and assessments of advanced chemical detection and personnel protection technologies to ensure DOE sites are effectively addressing the threat of terrorists using toxic industrial chemicals and chemical warfare agents during attacks; advanced friend/foe identification systems to minimize the potential for fratricide in close combat operations at DOE facilities; and several enhancements for DOE protective forces to include lightweight body armor to improve mobility, cooled vests to reduce heat stress, and night vision gear optimized for use in DOE critical facilities.

\# The Safeguards and Security program has been and will continue to be the key deterrent in preventing major incidents (i.e., theft, sabotage, terrorist activity, etc.) across the complex at 16 domestic weapons sites.

\# Enhanced training technology applications and applied a broader range of technologies to Departmental training, i.e., expanded use of interactive television, mobile training team, and televideo conferences to provide requisite training for a larger number of students without funding increases.

\# The Classification/Declassification program has played a key role in protecting our national security posture by identifying which information warrants protection in the interest of the nation's security, while at the same time providing public access to information which does not warrant protection. The program continues to implement P.L. 105-261, section 3161, discovering sensitive nuclear weapon design information (Restricted Data) embedded in other-agency records slated for declassification and release. The discoveries of Restricted Data, which are detailed informal reports to Congress, serve to protect such critical information from inadvertent release. The nation's security is preserved and the public's trust is

being rebuilt through implementation of this program. In FY 2000, funding for support service contracts supporting this program was provided in the Program Direction budget. Beginning in FY 2001, funding for this activity was budgeted in the Nuclear Safeguards and Security budget. However, for comparability purposes, FY 2000 funding for this activity is reflected in this budget's request.

\#   The DOE Information Security program continues support in analyzing and deterring major incidents involving the compromise of classified information. This includes expansion of information assurance forensics analysis capabilities to support investigations and prosecutions of unauthorized disclosures of classified information, expansion of the Technical Surveillance Countermeasures program, and providing input into the information security technology development program to develop new technology in response to growing concerns over unauthorized disclosures of classified information.

\#   The Cyber Security Office, within the Office of the Chief Information Officer, has developed and issued risk management based policies for the protection of both classified and unclassified information. Additionally, an expanded cyber security training effort was initiated, the incident response capability (Computer Incident Advisory Capability) was enhanced, and work was initiated on a Public Key Infrastructure strategy and the development of core cyber security architecture methodology and requirements.

\#   In FY 2001, the Communication Center and Special Facility were transferred from the Office of Emergency Management to the Office of the Chief Information Officer. In FY 2000 and FY 2001, this program was appropriated in the Emergency Management budget. However, for comparability purposes, FY 2000 and FY 2001 funding for this program is reflected in this budget's request.

\#   The Office of Critical Infrastructure Protection directs DOE's responsibilities under Presidential Decision Directive 63 to work with industry to develop and implement a plan to protect against, mitigate, respond to, and recover from attacks that would significantly disrupt the nation's energy infrastructure. The Office of Critical Infrastructure Protection is part of a Presidential crosscut coordinated by the Office of Science and Technology Policy.

Funding Profile

	FY 2000 Comparable Appropriation	FY 2001 Original Appropriation	FY 2001 Adjustments	FY 2001 Comparable Appropriation	FY 2002 Request
Nuclear Safeguards and Security					
Operational Support	31,638	37,359	-196	37,163	41,163
Technology and Systems Development . .	27,445	25,970		25,970	25,970
Classification/Declassification	17,067[a]	20,884	+66	20,818	20,818
Cyber Security	17,318[b]	30,339	-96	30,243	30,243
Critical Infrastructure Protection	2,100	3,000	-6	2,994	2,994
Subtotal, Nuclear Safeguards and Security	95,568	117,552	-364[c]	117,188	121,188
Less S&S General Reduction	-878				
Total, Nuclear Safeguards and Security . .	94,690	117,562	-364	117,188	121,188

(dollars in thousands)

---

[a]Reflects an increase of $400,000 from Reprogramming 99-R-20 for compliance with the FY 1999 Defense Authorization Act regarding inadvertent release of Restricted Data records during the automatic declassification of records under Executive Order 12958.

[b]Reflects funding increase of $8,000,000 received from an FY 2000 Supplemental request.

[c] Reflects funding decrease of $109,000 resulting from the allocation of a general reduction to Other Defense Activities and a decrease of $255,000 resulting from the FY 2001 Omnibus rescission.

Funding by Site

<div align="center">(dollars in thousands)</div>

	FY 2000	FY 2001	FY 2002	$ Change	% Change
Albuquerque Operations Office					
Los Alamos National Laboratory	6,688	5,272	6,658	+1,386	+26.3%
Sandia National Laboratories	9,718	10,325	10,714	+389	+3.8%
Pantex	20	215	270	+55	+25.6%
Albuquerque Operations Office	8,784	11,735	9,889	-1,846	-15.7%
Subtotal, Albuquerque Operations Office	25,210	27,547	27,531	-16	-0.1%
Ohio Field Office	100	140	100	-40	-28.6%
Chicago Operations Office					
Argonne National Laboratory	1,310	1,497	1,334	-163	-10.9%
Subtotal, Chicago Operations Office	1,310	1,497	1,334	-163	-10.9%
Idaho Operations Office	1,187	1,687	1,187	-500	-29.6%
Nevada Operations Office	1,216	1,428	1,478	+50	+3.5%
Oak Ridge Operations Office					
Oak Ridge Operations Office	3,435	2,441	2,212	-229	-9.4%
Oak Ridge National Laboratory		178	0	-178	-100.0%
Oak Ridge Institute for Science and Education	500	500	500	0	0.0%
Subtotal, Oak Ridge Operations Office	3,935	3,119	2,712	-407	-13.0%
Richland Operations Office	5,167	4,967	4,072	-895	-18.0%
Rocky Flats Area Office	0	140	0	-140	-100.0%
Oakland Operations Office					
Oakland Operations Office	2,500	2,500	3,900	+1,179	+43.3%
Lawrence Livermore Laboratory	11,176	11,247	14,192	+3,166	+28.7%
Subtotal, Oakland Operations Office	13,676	13,747	18,092	+4,345	+31.6%
Savannah River Site	1,743	2,560	2,418	-142	-5.5%
Washington Headquarters					
Office of Scientific and Technical Information	105	300	100	-200	-66.7%
Washington Headquarters	41,919	60,056	62,164	+2,108	+3.5%
Subtotal, Washington Headquarters	42,024	60,356	62,264	+1,908	+3.2%
Subtotal, Nuclear Safeguards and Security	95,568[a]	117,188[b]	121,188	+4,000	+3.4%
Less S&S General Reduction	-878				
Total, Nuclear Safeguards and Security	94,690	117,188	121,188	+4,000	+3.4%

[a]Reflects an increase of $400,000 from Reprogramming 99-R-20 for compliance with the FY 1999 Defense Authorization Act regarding inadvertent release of Restricted Data records during the automatic declassification of records under Executive Order 12958. Also reflects funding increase of $8,000,000 received from an FY 2000 Supplemental Request.

[b]Reflects funding decrease of $109,000 resulting from the allocation of a general reduction to Other Defense Activities and a decrease of $255,000 resulting from the FY 2001 Omnibus rescission.

Los Alamos National Laboratory

Work at Los Alamos National Laboratory (LANL) is designed to address current, evolving, and future needs, primarily in the areas of materials control and accounting (MC&A) and information security. Activities in MC&A include the development of measurement technologies and instrumentation to quantify difficult-to-measure or shielded special nuclear materials. LANL also develops standards for special nuclear materials to calibrate instruments around the complex. Other activities include evaluating commercial measurement systems and the development of MC&A training. Information security efforts are focused on developing a capability to perform classified processing across multiple platforms. Support is also provided to the Classification/Declassification program through the development and streamlining of classified guidance.

Sandia National Laboratories, NM

Sandia focuses on development of technologies and systems required to protect the Department from catastrophic consequences such as use of nuclear energy for malevolent purposes or the erosion of national security secrets through theft or diversion of classified materials or information. Technical assistance is provided for assessment of site vulnerability analysis and site safeguards and security plans. Support is also provided for the Declassification Productivity Initiative by providing automated tools that improve the efficiency of document classification/declassification reviews. The technology development program focuses on physical security technologies to secure the DOE complex. Activities include providing new detection capabilities to automatically detect unauthorized access, explosives, or other contraband. Sandia will develop advanced barrier technologies to prevent or substantially delay attacks. Technological solutions will also be provided to address new threats, such as chemical and biological weapons. In addition, Sandia will continue to maintain a core technical capability in interior and exterior sensors, alarm communications, access delay, and entry control. Assistance is also provided in developing comprehensive classification guidance for nuclear safety, environment, safety, and health and dismantlement/reuse; reviewing declassification proposals; and updating nuclear weapons classification guidance.

Pantex

Support was provided for the classification/declassification initiative by reviewing and releasing numerous documents prepared by the Amarillo National Resource Center for Plutonium (ANRCP). This also included classification training given to all cleared ANRCP employees.

Albuquerque Operations Office

The Nonproliferation and National Security Institute (NNSI), formerly called the Central Training Academy, is located in Albuquerque, New Mexico. NNSI was established to assist Headquarters DOE identify, implement, standardize, and monitor training programs in support of the Office of Safeguards and Security's program mission. NNSI's training curriculum, which consists of five core program elements (program management, personnel security, protection program operations, information security, and materials control and accountability), uses both traditional and distance learning technologies to provide onsite and facility training for safeguards and security personnel. The Classification/Declassification program is supported by developing computer-based training for certifying classifiers and declassifiers.

Ohio Field Office

The Ohio Field Office supports the Classification/Declassification program by conducting a large-scale declassification review program to ensure that all documents are properly classified or declassified prior to the scheduled closure of the facility in FY 2004.

Argonne National Laboratory

Argonne provides technical and programmatic development assistance in support of DOE's initiative to establish an effective national infrastructure assurance program that is supportive of, and harmonized with, national infrastructure assurance efforts. Argonne also supports database development for tasks associated for foreign ownership, control, or influence operations facilitating a database of information that ensures more thorough DOE investigation. Support is also provided for the Declassification Productivity Initiative by providing automated tools that improve the efficiency of document classification/declassification reviews.

Idaho National Engineering and Environmental Laboratory (INEL)

INEL provides Idaho-based field expertise, technical assistance, and engineering support for the development, review, evaluation, and implementation of security-related requirements to effectively meet DOE's goals and ensure cost-effective use of DOE dollars. This includes review and evaluation of security design requirements; engineering support for validation, justification, and site safeguards and security plan reviews; and development and refinement of security design criteria.

Nevada Operations Office

Activities will be conducted at the Remote Sensing Laboratory and the Special Technologies Laboratory, focusing on evaluating existing and new measurement technologies to determine their feasibility at DOE sites.

Efforts also include developing technologies to assist protective force personnel, including night vision goggles and investigating the use of ultraviolet tags to differentiate between the adversary and site personnel.

Oak Ridge, BWXT, Y-12

At Oak Ridge, technical assistance is provided for the development, maintenance, and conduct of courses and workshops that evaluate and ensure Information Systems Security certification; Master Safeguards and Security Agreement/Site Safeguards and Security Plan verification/validation; and physical protection systems. The technology development program provides support in physical security and material control and accounting addresses needs for protecting nuclear weapons, nuclear material, classified information, and other vital DOE assets (nonnuclear and unclassified). Expertise is provided in the document classification/declassification initiative and for classification guidance update and streamlining.

Oak Ridge National Laboratory (ORNL)

ORNL support is provided to the Classification/Declassification program by the declassification review of files, and the review of Calutron technology and proposal of UCNI topics for controlling sensitive information.

Oak Ridge Institute for Science & Education/Oak Ridge Associated Universities

At Oak Ridge, technical support provides implementation, training, operation, and quality assurance of the Personnel Security Assurance Program, and a variety of research and analysis activities in support of the personnel security function.

Richland Operations Office, Battelle Memorial Institute/Pacific Northwest National Laboratory (PNNL)

PNNL provides technical expertise, assistance, training, and awareness in support of information security. This includes the identification, inquiry, and resolution of security problems across DOE; and analysis of incidents and facility survey information. They also assist with the implementation of the Department's information assurance initiative and related activities to ensure effective and efficient identification of threats and vulnerabilities to DOE's distributed information and telecommunication systems. Technical assistance is provided that supports special nuclear material consolidation, Master S&S Agreement, Site S&S Plan support, and vulnerability assessment reviews and performance testing. PNNL provides technical, analytical, operation, and training support to the Systems Support Team for the Office of Foreign Visits and Assignments. The Classification/Declassification program is supported through development and streamlining of classification guidance.

Richland Operations Office, Fluor-Daniel Hanford

Provides Hanford-based field expertise, technical support and assistance for the review, update and consolidation of safeguards and security orders and policies and field guidance to cost effectively meet Department goals and objectives.

Rocky Flats Area Office

Rocky Flats provided support to the Classification/Declassification program by the review of documents containing information on various R&D activities at the site dating back to the early 1950's concerning the development and production of nuclear weapons. They also provided technical support in developing Headquarters classification guidance.

Lawrence Livermore National Laboratory (LLNL)

Technical support is provided to DOE's Information Systems Security Program for analysis and recommendations of policies, guidance, and information assurance tool development for all aspects of information systems security. The technology development program at LLNL is concentrated in information security, physical security, and MC&A. LLNL provides the Department with many tools to detect and respond to attacks to information system networks. The laboratory is developing a tool to automatically detect suspicious activities on computer networks and automatically provide a response capability. Physical security activities focus on providing software and interface upgrades to the Department's standardized alarm and access control system and evaluating low cost access control technologies for implementation throughout the DOE. In MC&A, measurement solutions for heterogeneous materials are being developed and implemented around the complex.

Oakland Operations Office

At Oakland, through the Computer Incident Advisory Capability (CIAC), provide round-the-clock cyber security incident response, analysis of cyber intrusions and attempted intrusions, and alert capability to DOE. Classification/declassification is supported through development and streamlining of classification guidance.

Savannah River Site

Work at Savannah River supports MC&A through the enhancement, development, deployment, and operation of a fully developed, ready to use, software application for nuclear materials accounting throughout the DOE complex. This technology will allow for greater reliability, efficiency, and cost savings through increased

standardization and use of advanced software technologies. The classification/declassification program is supported through the development and streamlining of classification guidance.

Office of Scientific and Technical Information

Support is provided for the classification/declassification initiative by improving the access capability to DOE's OpenNet data base and maintaining and enhancing the thesaurus and dictionary for the automated classification guidance system.

Washington Headquarters

The headquarters program for Nuclear Safeguards and Security has responsibility for implementation and oversight of the headquarters guard contract; the Safeguards and Security Information Management System (SSIMS) database; maintenance/upgrade of alarm systems, access control systems, and related computer equipment; and the protective force radio system; as well as the statutory-based responsibility for classifying and declassifying nuclear weapons-related technology (known as Restricted Data), ensuring that policies provide the public access to information necessary for an informed discussion of DOE's nuclear weapons program while continuing to support the paramount objective of protecting information from strategic adversaries, proliferants or potential proliferants, and terrorists. Specific areas covered are developing detailed classification guidance which specifically identifies information requiring protection in the interest of the national security; reviewing documents to classify information that still warrants protection and declassifying information that is no longer sensitive; training personnel both within DOE and throughout the Government to recognize Restricted Data information and to ensure that it is properly classified to prevent its inadvertent release; appraising DOE and other-agency classification and declassification programs to ensure policies and procedures are applied consistently; and developing state-of-the-art technology to make the classification and declassification process more efficient and effective. Also, in support of the Cyber Security program, support services are required to provide support to the DOE Headquarters staff in developing DOE-wide policies and plans, training, and architecture design and implementation.

Operational Support

Mission Supporting Goals and Objectives

Safeguards and Security (S&S) Operational Support provides essential technical and analytical expertise to ensure effective and efficient security; a protective force for Headquarters operations; reviews which ensure cost-saving measures in S&S throughout the Department; and standardized training responsive to the challenges of the changing post-cold war era. This support provides for the overall improvement of S&S activities.

Subprogram activities in this section of the budget include the following:

Nonproliferation and National Security Institute (NNSI) (formerly Central Training Academy) is the Center of Excellence for S&S training and training development. NNSI uses both traditional and distance learning technologies to provide onsite and facility training for S&S personnel ensuring that DOE maintains a well-trained workforce to protect the nation's vital nuclear and energy interests against espionage, sabotage or theft. NNSI assesses S&S field training needs and site training program performance and develops training courses to meet those needs. Distance Learning Training includes satellite transmission of NNSI training to multiple DOE sites and, through the use of modern interactive technology, allows each student to be part of the instructional process. Computer-based training, interactive audio/video training and correspondence courses are also provided.

Nuclear Materials Management and Safeguards Systems (NMMSS), which tracks and analyzes U.S. and Foreign nuclear activity, was transferred in FY 1999 from the International Nuclear Safeguards subprogram in the Office of Arms Control and Nonproliferation to the Office of Plutonium, Uranium, and Special Material Inventory in the Office of Security Affairs. In FY 2000 funding for NMMSS was provided within the Office of Arms Control and Nonproliferation. Beginning in FY 2001, NMMSS is funded in the Nuclear Safeguards and Security budget.

Information Security provides support across the Department in the areas of classified matter protection and control; technical security; operations security; and foreign ownership, control or influence. The accelerated information assurance program will provide a capability for ensuring that the resources and methods necessary to identify and prosecute unauthorized intruders of Departmental networks are effective and available. The information security activities will also provide a capability to evaluate proposed security measures within the Department's complex environment. The Information Security Resource Center (ISRC) incorporates technical expertise and professional development training to ensure that the five disciplines of information security function in an integrated, cohesive manner. The Technical Surveillance Countermeasures (TSCM) program, which is one of the five disciplines, ensures and enhances the security provided for Departmental facilities and programs in the greater Washington, D.C. area. The Information Security Protection Program provides a vehicle for providing technical expertise, assistance, and awareness training in information security disciplines. The information security program provides matrix support to various Departmental programs, such as the critical infrastructure program, the counterterrorism/ counterintelligence programs, and the cyber security program.

Security Education Briefings and Awareness provides support for Security Education Briefings and Awareness to reflect changing policies and procedures. Coordinates and participates in security education workshops and meetings for the exchange of resources and dissemination of security education information and assists contractors in establishing supporting briefing materials.

Personnel Security evaluates, reviews, and develops guidance and documents for use in evaluating the Personnel Security Assurance Program (PSAP) as it relates to medical, psychological, legal, security, and management components. Researches and prepares technical documents to support the Personnel Security activities. Provides technical assistance and operational support to the Personnel Security program manager to determine current status of science and technology in the component areas.

Headquarters **Guard Contract** provides security for the protection of Government property, classified matter, and personnel at headquarters buildings. The requested level arms the Security Officers above the 30% level, providing increased capability, skill, and authority above that of unarmed Security Officers.

Additional Support provides Headquarters and field elements with support to implement cost-saving S&S measures. This support includes technical assessments, risk management/vulnerability assessment expertise, engineering assistance, surveys, and performance testing. FY 2000 activities and funding levels were formulated to support risk management activities for high-value assets and to identify potential weaknesses and enhancements for protection systems and to incorporate lessons learned into the risk management processes. FY 2001 and FY 2002 will support continuing risk management issue resolution and the incorporation of greater sensitivity and capability into current vulnerability assessment tools. Additional Support also provides technical support for the development of physical security policies and programs and the security alarm system at Headquarters.

The Safeguards and Security Information Management System (SSIMS) tracks and reports classified S&S issues from all DOE field sites. SSIMS allows the Office of Safeguards and Security to conduct continuous reviews of the security measures in place at DOE/contractor facilities, ensuring compliance with DOE policy requirements and monitoring the effectiveness of Departmental policy involving the protection of national security assets. SSIMS funding will maintain the current database information system detailing facility findings, ratings, and general operational status.

Additionally, support continues for the implementation of a nuclear/biological/chemical weapons equipment program across the DOE complex to provide protection to the protective forces from these weapons of mass destruction.

Foreign Visits and Assignments Program (FV&A) manages the Department's program for granting access by foreign nationals to DOE federal and contractor (including National Laboratories) facilities to perform classified or unclassified work. The FV&A Program includes the responsibility to develop and promulgate DOE policy and procedures for reviewing and approving access; to develop and implement the Department's central documentation, reporting, and tracking information systems; to develop and coordinate responses to external requests (e.g., Congress) for information on the substance and numbers of foreign nationals visiting or working throughout DOE; and to support and assess operational results to

determine if identified national security requirements are being effectively addressed by the conduct of program operations. Additionally, the FV&A program is responsible for implementing the Department's Unofficial Foreign Travel policy and for continuing a partnership with the CFO to support the effective implementation of the Official Foreign Travel Order. The outcome objectives of the FV&A program are to provide a transparent capability to review and assure that program policy is effectively implemented in order to support delegation of approval authority at the lowest practical level of program operations and to implement a system of internal controls for vetting foreign national visitors and assignees based on a risk-assessment of the specific characteristics of the proposed visit or assignment. This internal control system requires a continuous quality improvement approach to foreign national vetting procedures and requirements and is ultimately capable of resolving the seemingly unresolvable conflicts between national security and open science.

Funding Schedule

	FY 2000	FY 2001	FY 2002	$ Change	% Change
	(dollars in thousands)				
Nonproliferation and National Security Institute (NNSI)	8,677	8,665	9,484	+819	+9.5%
Nuclear Materials Accountability Systems	2,500	2,500	4,938	+2,438	+97.5%
Information Security	4,269	4,814	4,814	0	0.0%
Security Education Briefing and Awareness	181	172	172	0	0.0%
Personnel Security	485	431	431	0	0.0%
Headquarters Guard Contract	7,654	9,000	10,419	+1,419	+15.8%
Additional Support	6,872	10,456	9,013	-1,443	-13.8%
Foreign Visits and Assignments Program	1,000	1,125	1,892	+767	+68.1%
Total, Operational Support	31,638	37,163[a]	41,163	+4,000	+10.8%

---

[a]Reflects a funding decrease of $60,000 resulting from the allocation of a general reduction to Other Defense Activities and a $136,000 decrease resulting from the FY 2001 rescission.

Detailed Program Justification

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Nonproliferation and National Security Institute (NNSI) . . .	**8,677**	**8,665**	**9,484**
# NNSI Operations	**8,614**	**8,602**	**9,421**

Conduct approximately 175 courses with 200 classroom iterations, emphasizing "Online Training," and course development to meet field site training needs for Weapons of Mass Destruction, chemical/biological equipment, and physical security systems. Additionally, FY 2002 supports new hire Security Police Officer training (SPO) for all field activities including upgrade of the Live Fire Range target systems to support new hire SPO training. Performance is measured by ability to meet planned number of training courses.

# NNSI Equipment	**63**	**63**	**63**

Provides funding to support NNSI's equipment-related needs such as replacement of outdated online and interactive television equipment.

Nuclear Materials Accountability Systems	**2,500**	**2,500**	**4,938**
# Nuclear Materials Management and Safeguards System (NMMSS) operational program	**2,500**	**2,500**	**2,500**

NMMSS is the national nuclear materials database, which also serves as the official nuclear material accounting system for DOE. It tracks and analyzes U.S. and foreign nuclear activity to satisfy statutory requirements and international obligations. Performance will be measured by the ability to maintain baseline measurement uncertainty information on Pu and HEU inventories while identifying where accountability information is inadequate.

# NMMSS upgrade			**1,400**

NMMSS will be upgraded off a technically obsolescent software platform. Increased functionality resulting from the upgrade will enable DOE to meet its expanded domestic and international nuclear material tracking needs. The upgrade will enable NMMSS to serve as a near-term technical solution for a corporate nuclear material information system to support all aspects of safeguards, nuclear material management, and inventory analyses. Performance will be measured by meeting scheduled upgrade milestones.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002

 # Local Area Network Materials Accounting System (LANMAS) **0** **0** **1,038**

Sustain an operationally capable LANMAS application software product suitable for production, installation, and operation in the DOE complex. This application, when installed on a suitable network system, will support all basic MC&A records and reporting functions required by DOE domestic and international policy.

Information Security **4,269** **4,814** **4,814**

 # Information Security Resource Center (ISRC) **1,602** **1,602** **1,602**

The ISRC in FY 2002 continues to provide technical expertise, assistance, training, and awareness in an integrated manner across the five disciplines of information security. This activity does not include cyber security functions. Activities support the identification of, inquiry into, and resolution of security problems across the Department, especially in the area of unauthorized disclosures and compromises of classified information; analysis of incidents and facility survey information to identify problems within the information security program; and analysis of foreign ownership, control or influence (FOCI) in determinations of contracts within the various program elements of DOE dealing in classified information. The funding level reflects the continuing need to sustain efforts to prevent unauthorized disclosures or compromises of classified information throughout DOE and the increasing complexity of FOCI issues.

 # Information Security Protection Program (ISPP) **1,405** **1,600** **1,600**

The Information Security Protection Program (ISPP) in FY 2002 continues to provide technical advice and awareness (excluding cyber security) to Departmental entities, excluding the National Nuclear Security Administration (NNSA). The ISPP provides unbiased capability in the areas of information security including technical vulnerability testing, design reviews to support the complex-wide Technical Surveillance CounterMeasures (TSCM) program, TSCM surveys and inspections at DOE sites not currently receiving such services, independent verification and validation of information security measures, TSCM equipment inspection support to international treaties, and awareness of emerging information security issues. ISPP activities provide a basic level of assurance that key assets are protected in a reasonable manner to ensure that national security concerns of the country are not adversely affected by adversary activities. Funding levels are based on attention to unauthorized disclosure of classified information and the conduct of TSCM services. This capability is also available to provide assistance to NNSA facilities.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002

 # Information Assurance and Forensics **1,100**   **1,450**   **1,450**

Activities include continuing information assurance forensics analysis capabilities to support investigations and prosecutions of unauthorized disclosures of classified information. Provide for training in new technologies and methods and the implementation of first responder training for the Department. Update and maintain the Grey List data base to allow contractors to submit foreign ownership, control or influence packages electronically, facilitating a data base of information that will ensure a more thorough DOE investigation. Maintain an internet accessible list of facility security offices for the more than 2,000 cleared DOE facilities and a list of classified mailing addresses for the over 500 facilities that are authorized to receive classified matter. Funding levels have been determined based on the rate of technological advances and, in the case of forensics, based on similar activities within the Department of Defense.

 # Technical Support **162**   **162**   **162**

Provides for continuation of on-site technical support for information security in the areas of technical reviews of technology transfer issues and the conduct of inquiries into unauthorized disclosures of classified information, emphasizing computer forensics.

Security Education Briefings and Awareness **181**   **172**   **172**

\# Provide training and security education awareness throughout the DOE complex through the management of the Security Education Special Interest Group (SE/SIG) and maintenance of the SE/SIG electronic bulletin board.

Personnel Security **485**   **431**   **431**

\# Operate Center for Human Reliability Studies
\# Support personnel security activities through guidance and product development, update and revise 90% of anticipated personnel security materials
\# Serve as technical liaison with Department of Defense (DOD) Personnel Security Research Center, DOD, Polygraph Institute and similar agencies and institutions
\# Upgrade and maintain Personnel Security Assurance Program (PSAP) electronic bulletin board; evaluate and modify 80% of needed PSAP training materials

Headquarters Guard Contract **7,654**   **9,000**   **10,419**

\# Ensure a sound protection program is offered to Headquarters employees and facilities through use of 40 static posts and roving patrols, 16 supervisors, 4 managers, and 6 instructors, receptionists and administrative assistants, armorer, quality assurance, badging and technical countermeasures personnel. In FY 2002, funding supports the arming of an additional 20 Security Police Officers and associated training, and unionization/escalation cost of the contract.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Additional Support	**6,872**	**10,456**	**9,013**

 # Safeguards and Security Information Management

System (SSIMS)	**300**	**300**	**700**

Support operational and basic maintenance costs for SSIMS which tracks and reports classified S&S issues from all DOE field sites. FY 2002 increase provides for development of standardized survey/inspection rating form in response to GAO Report on "Nuclear Security, Improvements Needed in DOE's S&S Oversight," installation of next generation Secure Terminal Equipment for encryption communication device upgrade, and cost increase of license renewals which includes expansion of classified system to new users.

# Alarm/Protective Force Radio Systems	**953**	**968**	**1,325**

In FY 2002, provides support and corrective/preventive maintenance of the Security Alarm and Access Control Systems (SAACS), magnetometers, x-ray machine, and executive protection and protective force radio systems. Increase will raise current operating funds above 1995 prices in order to sustain technical engineering support, provide maintenance and operation of the new ARGUS-based SAACS at a 100% operational level, and ongoing physical security upgrades at both headquarters facilities.

# Risk Management/Vulnerability Assessment	**1,593**	**1,733**	**1,733**

Provide risk management, vulnerability assessment, and safeguards and security system performance evaluations, verifications, and validations. FY 2002 funding level supports the implementation of the revised DOE standard vulnerability assessment tool suite. It also provides for onsite participation and field assistance for the most critical facilities' Site Safeguards and Security Plan development and review, Joint Tactical Simulation/Joint Conflict and Tactical Simulation, physical security system reviews, and S&S surveys. Performance is measured by identifying the need for S&S enhancements through the use of onsite evaluations and review of site S&S plans.

 # Technical Support for Physical Security Policies and

Programs	**387**	**387**	**387**

Evaluate the performance of integrated alarm management and control systems in the field to determine compliance with DOE directives, develop explosive detection performance evaluation test kits, revise DOE Definitions Guide, revise Protection Program Operations Survey Process, coordinate explosive detection technology workshops, and provide technical support in reviewing security system implementation at DOE sites.

# Lock replacement	**1,000**	**2,000**	**0**

Provided for the procurement and replacement of security locks meeting Federal Specification FF-L-2740A for containers holding sensitive classified material.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
# Vulnerability of Security Equipment	**1,000**	**0**	**0**

In support of Congressional initiative for FY 2000, assessed current vulnerability of security equipment throughout the DOE complex and developed solutions to identified vulnerabilities, i.e., evaluate current commercial security systems to determine applicability to DOE.

# Nuclear/Biological/Chemical Weapons (NBC) Protection Equipment, Training, and Chemical/Biological Detection Equipment	**0**	**3,429**	**1,829**

In response to U.S. Policy on Counterterrorism, provide a counterterrorist capability to detect, assess and protect Departmental facilities, employees and the environment from adversarial use of NBC as a weapon of mass destruction (WMD). FY 2002 reflects the funding necessary to complete implementation of NBC programs across the DOE complex. Funding level is based upon personal protection field testing, equipment modifications to enhance personnel survivability in potential NBC events, and complete explosive testing and equipment implementation. Performance will be measured by the Department's ability to meet the current and future spectrum of terrorist threats through enhancement of DOE's protective force and physical security capabilities; and demonstrated protective force counterterrorism response capability to the use of WMD through interagency exercises and training.

# Nondestructive Assay (NDA) Systems	**0**	**0**	**200**

Begin preparation of measurement control standards for safeguards NDA systems which measure special nuclear materials. Current NDA systems used by DOE have never been systematically evaluated to determine effects of inhomogeneity, impurities, packaging, etc., on assay bias and precision. This effort will ensure DOE's nuclear materials accounts are based on defensible measured values and protect nuclear materials in the U.S. from theft, loss, or illicit trafficking.

# Communications Center/Special Facility	**1,143**	**1,143**	**1,143**

The Communications Center provides all-source communications message traffic to all Headquarters elements, 24 hours a day, 7 days a week, and, as required, supports activities of the DOE Operations Center during the same time schedule. The Special Facility provides secure, national-level decision making capability for the Secretary of Energy, his advisors, and top level management.

# Equipment	**496**	**496**	**1,696**

Supports capitalized computer equipment requirements and modification and/or replacement parts to the Headquarters ARGUS-based SAACS. The increase in FY 2002 funding provides for exterior security improvements at the Forrestal facility as part of an ongoing effort to comply with recommended Department of Justice security upgrades at federal facilities.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Foreign Visits and Assignments (FV&A) Program	**1,000**	**1,125**	**1,892**

\# The FV&A program manages the Department's program for granting access by foreign nationals to DOE federal and contractor facilities to perform classified or unclassified work. Program scope also includes implementing solutions to issues and deficiencies identified by the General Accounting Office and Congress. In FY 2002, the program continues system automation, operational streamlining, and the risk-based "graded approach." Additionally, the FV&A program will implement an unrestricted access policy for fundamental science while assuring effective protection of national security interests, improve access decision support by the Foreign Access Centralized Tracking System (FACTS), initiate DOE-wide training to support deployment of the graded approach, implement recently assigned program responsibilities for Classified Foreign Visits & Unofficial Foreign Travel, and partner with the CFO to implement the Official Foreign Travel Order. Performance is measured by ability to provide an effective system for tracking and managing foreign visits at DOE facilities while supporting rapidly changing and growing national security needs.

Total, Operational Support	**31,638**	**37,163**	**41,163**

Explanation of Funding Changes from FY 2001 to FY 2002

	FY 2002 vs. FY 2001 ($000)

 # Nonproliferation and National Security Institute

Provide Security Police Officer (SPO) training for new hires including upgrade to Live Fire Range in support of SPO training and course development for identified field site training needs . . . . +819

 # Nuclear Materials Accountability Systems

- Upgrade system from outdated, DOS-based system . . . . +1,400
- Provide funding to sustain operationally capable LANMAS application software which will support all basic accountability and reporting required by DOE domestic and international policy when installed at sites . . . . +1,038

Total, Nuclear Materials Accountability Systems . . . . +2,438

 # Headquarters Guard Force

Allows for the arming of 20 additional guards and supports the unionization/escalation costs associated with the contract . . . . +1,419

 # Additional Support

- In support of SSIMS, develop a standardized survey/inspection form in response to a GAO report, install next generation Secure Terminal Equipment for encryption communication upgrade, and support license cost increase including expansion to new users . . . . +400
- Provide adequate funding for the Headquarters alarm system in order to maintain technical support and operate the ARGUS alarm system at 100% of capability. Funding has been stagnant since 1995 . . . . +357
- Reflects reduction for FY 2001 funding for procurement of security locks meeting Federal Specification FF-L-2740A . . . . -2,000
- Funding reduced to level of support necessary to complete implementation of Nuclear/ Biological/Chemical protection program . . . . -1,600
- Initiate development of measurement control standards for safeguards nondestructive assay systems for measuring special nuclear materials . . . . +200
- Provide equipment funding for exterior security improvements at the Forrestal facility in response to security upgrades recommended by Department of Justice . . . . +1,200

Total, Additional Support . . . . -1,443

	FY 2002 vs. FY 2001 ($000)

 # Foreign Visits and Assignments Program

Enhance the Foreign Access Centralized Tracking System (FACTS) and initiate DOE-wide training supporting the graded approach to current access policy while assuring effective protection of national security interests . . . .   +767

Total Funding Change, Operational Support . . . .   +4,000

Technology and Systems Development

Mission Supporting Goals and Objectives

The Technology Development Program's mission is to develop new technologies or modify commercial systems to protect the national nuclear weapons complex, special nuclear materials, classified information and other critical assets. The threats facing DOE facilities and sites continue to evolve and present many challenges to the Department. Traditionally, the Technology Development Program was concerned with the protection, control, and accounting of nuclear materials and weapons against threats such as weapons of mass destruction, terrorism, cyber attacks and the insider. The weaponry and sophistication of these threats continue to present an increasing challenge that must be offset by improved technologies. Although the Department is no longer in the production mode, it is disassembling nuclear weapons being returned from DOD, and accepting weapons grade materials from other countries. All of these weapons components and materials have resulted in increased nuclear material inventories which the Department must properly account for and protect. Technology continues to be the key in meeting these increased requirements, and in the continued protection of facilities and national security assets in a cost effective manner. Safeguards and security deficiencies and vulnerabilities requiring technical solutions have been identified and validated by security managers assigned to field offices throughout the complex. Currently, funding permits only part (approximately 40%) of these requirements to be addressed by technology development projects intended to mitigate specific vulnerabilities. The program will strive to sustain and utilize core security technologies and expertise that are not only capable of producing new technical solutions, but also providing critical design guidance as new facilities are being designed, built or rehabilitated.

The Technology and Systems Development program is divided into the following subprograms:

Science and Technology Development Projects - includes all activities ranging from basic research to full scale development and modification of available technology for S&S applications.

Technology Application - includes site implementation of a technology or system that will address an S&S deficiency, and technology transfer to a qualified manufacturer.

Technology Support, Assistance, and Consultation Tasks - includes technical training, technical support to Headquarters, technical workshops and seminars, and technical support and assistance to the DOE complex.

Each subprogram is concentrated in the following disciplines:

Physical Security - Activities are focused on intrusion detection, access control, alarm control and display, alarm assessment, adversary barriers/delay, and protective force equipment.

Material Control and Accounting - Efforts are focused in nuclear material measurements, material accounting, material control, training, and statistical control methods.

Information Security - Projects are focused on computer network intrusion/attack detection tools, technical assistance, system integration, and information assurance.

Funding Schedule

	(dollars in thousands)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Science and Technology Development Projects	24,129	24,400	24,400	0	0.0%
Technology Application	1,066	805	805	0	0.0%
Technology Support, Assistance, and Consultation Tasks	2,250	765	765	0	0.0%
Total, Technology and Systems Development	27,445	25,970	25,970	0	0.0%
Crosswalk of Disciplines					
Physical Security	11,878	13,275	14,972	+1,697	+12.8%
Material Control and Accounting	9,297	9,867	8,954	-913	-9.3%
Information Security	6,270	2,828	2,044	-784	-27.8%
Total	27,445	25,970	25,970	0	0.0%

**Other Defense Activities/Security and Emergency Operations/
Nuclear Safeguards and Security/Technology and Systems
Development**

FY 2002 Congressional Budget

Detailed Program Justification

<table>
<tr><td></td><td colspan="3">(dollars in thousands)</td></tr>
<tr><td></td><td>FY 2000</td><td>FY 2001</td><td>FY 2002</td></tr>
<tr><td>**Physical Security** . . . .</td><td>**11,878**</td><td>**13,275**</td><td>**14,972**</td></tr>
<tr><td># **Physical Security Technological Solutions** . . . .</td><td>**7,898**</td><td>**9,120**</td><td>**11,257**</td></tr>
</table>

Develop new capabilities such as an improved version of the ASSESS vulnerability analysis software tool, which will be called ATLAS (Adversary Timeline Analysis System); self healing and activated barriers to offset vulnerabilities associated with physical barriers; enhancements to ARGUS our central alarm, access control, and command station; video loss and tamper detection; and other capabilities to mitigate specific threats and vulnerabilities. Continue to provide technical support to the DOE complex. Increased funding provides protection measures for security components to survive hostile directed energy environments, and provides a team of experts to perform on-site assessments and modeling of security systems in a hostile chemical environment. (SNLA, LLNL, Special Technologies Laboratory, ORNL, Remote Sensing Laboratory). Performance will be measured by the ability to modify current protection components, or develop new technologies for S&S applications to partially address approximately 40% of documented and validated field user needs.

<table>
<tr><td># **Performance Testing** . . . .</td><td>**2,000**</td><td>**2,175**</td><td>**2,000**</td></tr>
</table>

Conduct performance testing of security equipment such as intrusion detection, video assessment, entry control, biometrics, barriers and access delay systems, chemical agent protection equipment, etc., so that the test data can be used by the ATLAS vulnerability assessment software, the joint tactical simulation force-on-force modeling tool, and by DOE field users that must make procurement decisions. (SNLA, LLNL, ORNL)

<table>
<tr><td># **Technical Support Working Group** . . . .</td><td>**1,500**</td><td>**1,500**</td><td>**1,142**</td></tr>
</table>

Provide input to the counter terrorism community's Technical Support Working Group, which helps DOE gain technological leverage, develop required security technologies, and provide DOE input to significant DOD and counterterrorism community investment. Funding decrease is to support increased efforts in the development of physical security technological solutions. (SNLA, LLNL)

<table>
<tr><td># **Capital Equipment** . . . .</td><td>**480**</td><td>**480**</td><td>**573**</td></tr>
</table>

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002

Material Control and Accounting (MC&A) **9,297**   **9,867**   **8,954**

**Special Nuclear Material Measurement Technologies** **6,933**   **7,653**   **7,140**

Develop analysis and detection capabilities for alternate nuclear materials (americium and neptunium), foreign research reactor spent nuclear fuels, dismantled weapons components, and large volumes of difficult to measure nuclear materials to account for DOE's total nuclear materials inventory. Develop special nuclear materials standards to calibrate instruments, miniature measurement systems to quantify hold-up materials in process plant piping previously unaccessible, and more efficient assay technologies that will reduce operations cost and decrease personnel exposure to nuclear materials. Provide technical assistance to operations facilities in support of newly fielded technologies. Decrease is a result of funds being shifted to developing technological solutions that address increased vulnerabilities in physical security systems. (LANL, LLNL)

**Special Nuclear Material Control Technologies** **800**   **850**   **800**

Efforts are focused on confirming the presence of special nuclear materials in storage to prevent and detect unauthorized access or removal of the materials. Technologies under development include active and unattended vault monitoring systems, active seals and tags, and emergency exit radiation monitors. Decrease is a result of funds being shifted to developing technological solutions that address increased vulnerabilities in physical security systems. (SNL, BWXT)

**Nuclear Material Accounting** **1,200**   **1,000**   **650**

Provide required modules to the Local Area Network Material Accounting System (LANMAS), the Department's standard material control and accounting system; develop automatic tools to perform statistical analyses on inventory data. Decrease reflects a completion of key functions. (SRS, LANL)

**Capital Equipment** **364**   **364**   **364**

Information Security **6,270**   **2,828**   **2,044**

**Automated Information Security Tools** **6,085**   **2,735**   **2,044**

Develop tools that automatically detect unauthorized access to DOE security systems and provide the appropriate response; provide asset tracking technologies that automatically detect unauthorized removal of electronic media; and develop effective, low-cost computer based training for DOE system administrators. Decrease is a result of funds being shifted to developing technological solutions that address increased vulnerabilities in physical security systems. (Special Technologies Lab/LLNL, LANL, PNNL)

**Capital Equipment** **185**   **93**   **0**

Total, Technology and Systems Development **27,445**   **25,970**   **25,970**

Other Defense Activities/Security and Emergency Operations/
Nuclear Safeguards and Security/Technology and Systems
Development   **FY 2002 Congressional Budget**

Explanation of Funding Changes from FY 2001 to FY 2002

	FY 2002 vs. FY 2001 ($000)

 # Physical Security

Increased emphasis is on providing protective measures for security components to assure survival in hostile directed energy environments; on-site assessments of entire security systems in an environment involving lethal chemical agents; and activated denial systems to offset vulnerabilities associated with physical barriers.. . . . .   +1,697

 # Material and Control and Accounting (MC&A)

Reflects shift in funding to the development of technological solutions to address increased vulnerabilities in the area of Physical Security. . . . .   -913

 # Information Security

Reflects shift in funding to the development of technological solutions to address increased vulnerabilities in the area of Physical Security. . . . .   -784

Total Funding Change, Technology and Systems Development   0

Classification/Declassification

Mission Supporting Goals and Objectives

The Department of Energy has a unique statutory-based responsibility for the classification and declassification of nuclear weapons-related technology, known as Restricted Data. In that regard, the Classification/Declassification program's mission is to identify which of the Department's information warrants protection in the interest of national security and which information does not warrant protection. This critical program is truly a corner stone of the U.S. nuclear nonproliferation and security program since an asset cannot be protected until it is identified as requiring protection. Consistent with this mission, the Classification/Declassification program funds Management and Operating Contractors in the field and Support Service Contractors at Headquarters who provide highly technical support in a number of ways: by conducting declassification reviews and audits of documents under Statute and Executive order to identify information warranting protection from strategic adversaries, proliferants or potential proliferants and terrorists, while declassifying information critical to public discourse on the direction of the nuclear weapons program into the next century; by developing detailed classification guidance to increase the Government-wide understanding of which information requires protection in the interest of the nation's security; conducting training of personnel and appraisals of classification/declassification programs throughout Government to ensure consistent protection of the nation's most sensitive information; and by developing state-of-the-art technology to enhance the classification and declassification process, making it more efficient and effective.

Funding Schedule

	(dollars in thousands)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Classification/Declassification	17,067[a]	20,818[b]	20,818	0	0%

---

[a]Reflects an increase of $400,000 from Reprogramming 99-R-20 for compliance with the FY 1999 Defense Authorization Act regarding inadvertent release of Restricted Data records during the automatic declassification of records under Executive Order 12958.

[b]Reflects a funding decrease of $20,000 resulting from the allocation of a general reduction to Other Defense Activities and a $46,000 decrease resulting from the FY 2001 Omnibus rescission.

Detailed Program Justification

(dollars in thousands)

	FY 2000	FY 2001	FY 2002
# Declassification Reviews	**8,740**	**11,250**	**11,250**

Declassification review of documents under statutory requirements (i.e., P.L. 105-261, National Defense Authorization Act for Fiscal Year 1999, P.L. 106-65, National Defense Authorization Act for Fiscal Year 2000, the Freedom of Information Act) or Executive order requirements (i.e., Executive Order 12958, Classified National Security Information). Reviews are designed to protect sensitive nuclear weapon information from inadvertent public release throughout the Government, and to release to the public all documents not warranting protection in the interest of the nation's security.

	FY 2000	FY 2001	FY 2002
# Classification Reviews	**1,166**	**1,500**	**1,500**

Classification review of newly created documents to determine which documents contain information warranting protection in the interest of the national security, e.g., sensitive nuclear weapon design information. Reviews are required under statutory, Executive Order, litigation and Congressional requirements.

	FY 2000	FY 2001	FY 2002
# Classification/Declassification Training and Appraisals	**960**	**1,184**	**1,184**

Conduct training of personnel and appraisals of classification/declassification programs both internally and for other agencies. Training and appraisal programs are designed to provide consistent protection throughout the Government for sensitive nuclear weapon information, as mandated in P.L. 105-261, and 10 CFR Part 1045, Nuclear Classification and Declassification.

	FY 2000	FY 2001	FY 2002
# Classification Guidance Program	**3,135**	**3,198**	**3,198**

Maintain comprehensive classification guidance program to identify information which requires protection in the interest of national security. FY 2002 continues guidance system streamlining initiative, increasing the scope of the administrative/policy guidance, issuing weapon design and science guidance in the streamlined format, and designing the balance of system ($998). As programmatic needs arise, will update existing classification topics and develop new topics ($2,200). Performance will be measured by continued declassification guidance streamlining and issuance of additional guides in streamlined format.

	FY 2000	FY 2001	FY 2002
# Document Declassification Technology Development	**3,066**	**3,686**	**3,686**

Develop state-of-the-art technology for document declassification to improve efficiency and effectiveness of declassification, and to protect classified information from disclosure. In FY 2000, set up test capability at one field location. Expand the system to multiple field sites in FY 2001 and FY 2002, including on-site testing and implementation. Transform paper guidance and human knowledge into machine readable format.

	FY 2000	FY 2001	FY 2002
Total, Classification/Declassification	17,067	20,818	20,818

Cyber Security

Mission Supporting Goals and Objectives

The goal of the Cyber Security Program is to provide consistent principles and requirements that line management can implement for the protection of classified and unclassified information used or stored on Departmental Information Systems, as required by national level laws and policies. The policies for the protection of this information will ensure that classified and unclassified information is protected consistently across the various elements of the Department in a cost-effective manner, and consistent with the protection of this information in paper form.

The program will also provide for Departmental cyber security tools and capabilities that are required by all Departmental elements. These tools and capabilities are primarily training requirements, incident response capability, and core cyber security architecture development and deployment.

The Cyber Security Program has four major objective areas:

Policy and Planning – To provide high level consistent, risk management-based policies and implementation guidance for the protection of cyber assets.

\# **Training** – to provide consistent core training requirements for cyber security professionals, system administrators, senior management, and general users.

\# **Operations** – to provide Departmental capabilities for cyber incident response, core cyber security architecture, cyber intrusion detection and reporting, and Public Key Infrastructure (PKI) architecture.

\# **Technical Development** – to provide technical tools to eliminate cyber security vulnerabilities where commercial or Government products are not available.

Funding Schedule

	FY 2000	FY 2001	FY 2002	$ Change	% Change
(dollars in thousands)					
Policy and Planning	2,040	2,000	3,000	+1,000	+50.0%
Training	1,000	3,350	1,000	-2,350	-70.1%
Operations	13,278	23,314	24,743	+1,429	+6.1%
Technical Capability	1,000	1,579	1,500	-79	-5.0%
Total, Cyber Security	17,318[a]	30,243[b]	30,243	0	0.0%

Detailed Program Justification

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Policy and Planning	**2,040**	**2,000**	**3,000**

Develop and maintain policies and working documents necessary to provide the framework for an integrated Cyber Security Program across the Department's varying missions and sites. Review Implementation Plans and provide guidance to the Departmental sites on the execution of cyber security programs detailed in the Cyber Security Program Plans (CSPPs). Expand analysis capabilities of the CSPP database in order to baseline the Department's cyber security posture. Continue to update and implement the Cyber Security Program Action Plan, which describes ongoing and future activities under the DOE Cyber Security Program. The Action Plan is a living document that lays out an integrated set of activities over a two-year period and provides a foundation for budget planning and program execution. Performance measure will be the implementation of the Cyber Security Program Action Plan.

[a]Reflects funding increase of $8,000,000 received from an FY 2000 Supplemental request.

[b]Reflects funding decrease of $29,000 resulting from the allocation of a general reduction to Other Activities and a $67,000 decrease resulting from the FY 2001 Omnibus rescission.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Training	**1,000**	**3,350**	**1,000**

Conduct comprehensive training program. In FY 2000, completed Phase I training for a limited number of people and conducted baseline skills evaluation and certification for classified computer security. In FY 2001, implemented DOE-wide training to a broad audience based on the Comprehensive Training Strategy and continued baseline skills evaluation and certification for classified computer security. Identified two System Administration, Networking, and Security (SANS) training courses that met the immediate needs of the Department and offered the courses on-line to over 5,000 federal and contracted employees. This included, but was not limited to managers, system administrators, cyber security professionals, and general users. In FY 2002, will continue baseline skills evaluation and certification and will offer comprehensive training to a limited audience of DOE employees and contractors with access to DOE classified and unclassified computer systems. The Comprehensive Cyber Security Training Program will continue to use commercial and government off-the-shelf materials whenever possible. Performance will be measured by providing cyber security education, training, and awareness for individuals responsible for implementing cyber security and protective measures.

Operations	**13,278**	**23,314**	**24,743**

Provide for continued cyber security incident response capabilities, DOE-wide implementation of baseline cyber security architecture, and enhanced Public Key Infrastructure (PKI) deployment.

# Computer Incident Advisory Capability (CIAC) at LLNL . .	**5,537**	**5,000**	**7,000**

In FY 2000, provided support for a total of 15 contractor FTEs to provide cyber security incident response, analysis of cyber intrusions and attempted intrusions, and warning capability for the Department. FY 2000 provided partial year funding for support. In FY 2001, CIAC received FY 2000 Supplemental funding in addition to FY 2001 appropriation to ramp up to 25 FTEs. In FY 2002, will maintain contractor support level at 25 FTEs. FY 2001 and 2002 reflect full year funding. Performance will be measured by ability to maintain a centralized incident response capability to provide incident analysis of cyber intrusions and attempted intrusions, and warning capability for all DOE sites.

# Cyber Security Core Architecture Engineering and			
Deployment	**6,964**	**15,696**	**10,443**

FY 2000 supported evaluation of the baseline cyber security capability at individual field sites. In FY 2001, implemented cyber security architecture upgrades throughout the complex as prioritized according to risk and necessity. Field architecture upgrades were funded with FY 2000 Supplemental and FY 2001 appropriations in two phases in FY 2001. In FY 2002, will continue cyber security architecture upgrades across the DOE complex. Performance will be measured by the implementation of cyber security architecture upgrades across the DOE complex.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
# Classified Systems Support	**300**	**618**	**300**

Provide funding for Independent Validation and Verification (IV&V) for accreditation of classified systems. In FY 2001, funding also provided for a classified DOE information server. FY 2002 provides for continued IV&V of classified systems.

# PKI Initiative	**477**	**2,000**	**2,000**

Provide funding to operate and expand inter-site PKI capability for the protection of unclassified data in transit, as well as the protection of unclassified data in storage. FY 2001 funding provides for Departmental infrastructure to support token or biometric authentication, allowing for coordination and unification of previously independent PKI efforts. Will expand inter-site PKI capability to several Field sites in FY 2002.

# STU-III Replacement	**0**	**0**	**5,000**

In FY 2002, will begin initiative to replace the Department's Secure Terminal Unit (STU-III) devices with Secure Terminal Equipment (STE) secure voice/data transmittal devices, as required by Advisory Memorandum COMSEC 2-98. National direction requires that incremental replacement of the current STU-III equipment occur through FY 2005. DOE has opted for a 25 percent per year replacement rate during the allotted time period. Supplemental Program Direction[c] funding has been provided in FY 2001 for preliminary testing of STE devices.

Technical Capability	**1,000**	**1,579**	**1,500**

Provides funding for technical support and minimal R&D efforts. Funding in FY 2000 and 2001 supported the establishment of limited testing capability for commercial off-the-shelf (COTS) cyber security products prior to deployment throughout the Department. FY 2001 funding also provided for network intrusion detection R&D, connection log analysis, and multiplatform trusted copy software enhancements. In FY 2002, there is a continued need to evaluate and potentially modify COTS cyber security products to ensure that the application of these products does not significantly interfere with primary organizational or computer missions, and to identify weaknesses in COTS products that must be mitigated to ensure a consistent cyber security implementation

Total, Cyber Security	**17,318**	**30,243**	**30,243**

Explanation of Funding Changes from FY 2001 to FY 2002

	FY 2002 vs. FY 2001 ($ 000)

 # Policy and Planning

Maintain policies for an integrated Cyber Security Program; review and analyze Cyber Security Program Plans being developed at Departmental sites . . . . +1,000

 # Training

Maintain oversight responsibility of the Cyber Security Training Program, but only minimally fund courses offered Department-wide . . . . -2,350

 # Operations

- Provide full year funding to maintain M&O contractor support at 25 FTEs . . . . +2,000

- Decrease funding for cyber security architecture upgrades due to a curtailed need for the Chief Information Officer to supplement funding for procurement of architecture equipment in the field . . . . -5,253

- Provide for IV&V, but discontinue CIO funding for the classified information server at LANL . . . . -318

- Initiate STU-III replacement by replacing 25% of existing STU-III secure voice/data devices with STE devices, as required by Advisory Memorandum COMSEC 2-98 . . +5,000

Total, Operations . . . . +1,429

Technical Capability

Decrease funding for R&D projects . . . . -79

Total Funding Change, Cyber Security 0

Critical Infrastructure Protection

Mission Supporting Goals and Objectives

The nation's energy infrastructure—composed of increasingly interdependent industries that produce and distribute electric power, natural gas, and petroleum fuels—is undergoing rapid and dramatic change. It is also experiencing unprecedented and increasingly frequent problems. This is particularly evident in California, where curtailments, rolling blackouts, and escalating power bills are becoming the norm. Similar but less severe problems are occurring throughout the West and in other regions of the country. Many of these problems can be traced to increasing energy demands, generating capacity shortfalls, transmission and environmental constraints, the way deregulation initiatives are being implemented, planned and unplanned outages of key energy components (e.g., generating facilities, gas pipelines), interdependencies among the energy and other critical infrastructures, wholesale power pricing fluctuations, and other market forces.

The security, economic prosperity, and social well being of the nation depend on the reliable functioning of not only the energy infrastructure, but also the other critical and increasingly interdependent infrastructures. These include telecommunications, water supply systems, transportation, banking and finance, and emergency and government services. In the new economy, these interconnected infrastructures have become increasingly fragile and subject to disruptions that can have broad regional consequences.

For these reasons, sustaining the robustness and resilience of the energy infrastructure, which is the lifeblood of these interdependent infrastructures, is essential. To do this, infrastructure owners and operators; Federal, state, and local governments; consumers; and other stakeholders must improve their understanding of (1) the forces at work that may cause a prolonged energy crisis that could impact infrastructures and services and (2) strategies and technologies to protect against, mitigate the effects of, respond to, and recover from energy infrastructure disruptions.

The urgency of this mission cannot be stressed too strongly, particularly in light of the current energy crisis in California and the West. The energy infrastructure today is in the midst of significant change and is increasingly under stress. Operations and business practices now rely on automated systems and the Internet. At the same time, reliability is being impacted by structuring, deregulation, downsizing, inadequate and aging systems, regulatory constraints, a fall-off in research and development, and lack of incentives to make necessary infrastructure upgrades. The net result is that the nation is facing potential energy infrastructure disruptions that will have broad regional impacts over the next two years.

Funding Schedule

<div align="center">(dollars in thousands)</div>

	FY 2000	FY 2001	FY 2002	$ Change	% Change
Critical Infrastructure Protection	2,100	2,994^a	2,994	0	0.0%

Detailed Program Justification

<div align="center">(dollars in thousands)</div>

	FY 2000	FY 2001	FY 2002
# **Infrastructure Interdependencies**	**1,100**	**1,523**	**1,523**

Infrastructure Interdependencies: The energy infrastructure is highly interdependent internally and with other infrastructures. This work will use modeling and simulation to characterize the interdependencies, quantify the impacts of vulnerabilities in each system on the others, and rank the order of importance of various interdependencies. Work will focus on developing, demonstrating, and delivering analytic capabilities and supporting knowledge bases to improve significantly the understanding of and the ability to study comprehensively the interdependent nature of the National energy infrastructure. Over a 6-year time span, this will involve (1) enhancing existing and developing new analytical tools that treat infrastructure interdependencies explicitly; (2) enhancing early alert screening tools that provide infrastructure stress indicators; (3) coordinating with Federal Agencies to link to models and simulations of other critical infrastructures; (4) enhancing existing and developing new policy and impact analysis tools; and (5) developing an integrated architecture for analyzing the technical, economic, and national security implications of energy technology and policy decisions. Performance Measure: Develop and identify DOE technologies and approaches that can help assure our nation's critical energy infrastructures and facilitate their use by the private sector and other Federal agencies.

---

^aReflects funding decrease of $6,000 resulting from the FY 2001 Omnibus rescission.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
# Industry Outreach and Vulnerability Assessment	**1,000**	**1,471**	**1,471**

Industry Outreach and Vulnerability Assessment: Provides expert technical assistance to the Energy Sector Coordinators in establishing collaborative working relationships between the government and the energy industry and other stakeholders; facilitates development of information collection and sharing and assists in analyses. The Infrastructure Assurance Outreach Program focuses on developing an understanding of the vulnerabilities of operations of the very large, integrated, and complex electric power, natural gas, and oil systems and the relationship of information flows to operational capabilities. A related area of focus is concerned with high-security Supervisory Control and Data Acquisition (SCADA) systems to address the issues of secure communications, validation of commands, and the development of design and operational guidelines, including authentication and authorization techniques to control access to energy system commercial information. FY 2002 activities will continue infrastructure assurance efforts in electric power, oil, and natural gas infrastructures, working with utilities and state and local governments to identify and evaluate the threats to and vulnerabilities of the National energy infrastructure. Focus will be on developing and implementing regional infrastructure approaches and plans. This includes both cyber (information) and physical infrastructure components. A summary of lessons learned and recommended security practices for the energy industry will be augmented. Performance Measure: Work with the national energy sector toward developing the capability for assuring the nation's energy infrastructures, including identifying the physical and cyber vulnerabilities and interdependencies of the electric power, oil, and gas infrastructures.

Total, Critical Infrastructure Protection	**2,100**	**2,994**	**2,994**

Other Defense Activities/Security and Emergency Operations/Nuclear Safeguards and Security/Critical Infrastructure Protection

FY 2002 Congressional Budget

Capital Operating Expenses and Construction Summary

	FY 2000	FY 2001	FY 2002	$ Change	% Change
Total, Capital Equipment	1,496	1,496	2,696	+1,200	+80.2%

Security Investigations

Program Mission

The Security Investigations Program funds background investigations for all Department of Energy (DOE) federal personnel and contractors who, in the performance of their official duties, require access authorizations for Restricted Data, National Security Information, or certain special nuclear material.

Program Goal

Support the common defense and security of the United States by ensuring that only appropriate personnel are determined to be eligible for access to classified information, special nuclear material, or occupy sensitive positions.

Program Objectives

\#   Ensure the timely and efficient processing of approximately 22,756 personnel security investigations needed for initial access authorizations and reinvestigations for the DOE complex.

\#   Review the types and numbers of investigations to ensure consistency with DOE mission changes, considering heightened security requirements.

\#   Ensure that the quality of an investigative product is sufficient for DOE security needs.

Significant Accomplishments and Program Shifts

\#   In FY 2001, funding for field non-federal employees' security investigations, excluding those from the Office of Naval Reactors, will be directly funded in the Security Investigations budget rather than from the program office budgets for the first time since FY 1998.

\#   As a result of the Defense Authorization Act for Fiscal Year 2000 (S.1059, Section 3144), there has been a change in policy requiring personnel in positions that are of such a critical nature that any compromise could gravely impact U.S. national security to have background investigations conducted by the Federal Bureau of Investigation (FBI). People in less sensitive positions will continue to have their investigations performed by the Office of Personnel Management (OPM).

\#   The FBI reduced their case prices in FY 2001 from $4,500 to $3,395 for an initial investigation and from $3,000 to $2,675 for a reinvestigation. FBI cases are still priced considerably higher than investigations performed by OPM.

\#   In FY 2001, the Security Investigations budget was appropriated $33 million. Prior-year carryover of $8.2 million is available to supplement the appropriated funds. This amount of carryover was largely due to the inability to move program funds where needed. Restrictions on the use of investigative funds for federal employees did not permit those funds to be used for contractor employee investigations. Also, program funds could not be moved from one site to another and the FBI restricted the number of investigations DOE could submit. The program will avoid major funding shortages for investigations in FY 2001 with the use of prior-year funding, however, there will be no prior-year carryover to fall back on in FY 2002.

\#   In order to ensure that the number of security clearances is consistent with mission requirements, the number of "Q" access authorizations will increase in FY 2001 due to heightened security requirements and Congressional add-ons to the Weapons Appropriation which will accommodate a larger work force for the Defense Programs mission.

\#   In FY 2002, the "Q" reinvestigation workload is projected to be significantly higher (approximately 2,314 more cases) than budgeted for in FY 2001. The Department considers reinvestigations a priority over initial investigations, which means less funding ($6.5M) will be available for initial investigations compared to the previous fiscal year.

\#   After 5 years of practically no activity, "L" reinvestigations will be resumed, which accounts for 1,642 of the additional 1,795 National Agency Checks (NAC's) required in FY 2002. (The reinvestigation interval for "L" access authorizations, which requires a NAC, changed from 5 to 10 years in March 1997).

Funding Profile

	FY 2000 Comparable Appropriation	FY 2001 Original Appropriation	FY 2001 Adjustments	FY 2001 Comparable Appropriation	FY 2002 Request
	(dollars in thousands)				
Estimated Appropriation Distribution					
National Nuclear Security Administration	14,138	17,358		17,358	25,966
Defense Environmental Management	7,037	8,485		8,485	9,210
Science	1,183	1,171		1,171	1,371
Nuclear Energy	2,555	0[a]		0[a]	0
Security & Emergency Operations	12,664	5,986	-73[b]	5,913	8,380
Subtotal, Security Investigations	37,577[c]	33,000	-73[b]	32,927	44,927
Less additional allocation from other program funds	-4,913	0	0	0	0
Total, Security Investigations	32,664	33,000	-73[b]	32,927[d]	44,927

Public Law Authorization:

Public Law 83-703, "Atomic Energy Act of 1954"

---

[a]Beginning in FY 2001, security investigations for non-federal personnel at Naval Reactors sites will be budgeted for in the Naval Reactors Development budget.

[b]Reflects Omnibus rescission of $73 thousand assigned to this program.

[c]Reflects Government-wide decrease of $336 thousand pursuant to FY 2000 Consolidated Appropriations Act rescission assigned to this program, and an increase of $4.913 million to allocate other program funds for security investigations of field non-federal employees.

[d]Does not reflect the use of at least $8.2 million in prior-year carryover.

Funding by Site

		(dollars in thousands)			
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Albuquerque Operations Office	10,638	12,512	19,492	+6,980	+55.8%
Chicago Operations Office	486	504	642	+138	+27.4%
Idaho Operations Office	495	690	787	+97	+14.1%
Nevada Operations Office	1,057	918	2,099	+1,181	+128.6%
Oak Ridge Operations Office					
Oak Ridge Operations Office	4,548	4,583	4,610	+27	+0.6%
Oak Ridge Institute of Science & Education.	150	150	175	+25	+16.7%
Total, Oak Ridge Operations Office	4,698	4,733	4,785	+52	+1.1%
Pittsburgh Naval Reactors Office	1,795	0[a]	0	0	0.0%
Richland Operations Office	1,325	2,125	1,355	-770	-36.2%
Oakland Operations Office	2,180	3,168	4,843	+1,675	+52.9%
Savannah River Operations Office	2,479	3,264	3,734	+470	+14.4%
Schenectady Naval Reactors Office	660	0[a]	0	0	0.0%
Washington Headquarters	11,764	5,013	7,190	+2,177	+43.4%
Subtotal, Security Investigations	37,577[b]	32,927[c]	44,927	+12,000	+36.44%
Less additional allocation from other program funds	-4,913	0	0	0	0.0%
Total, Security Investigations	32,664	32,927	44,927	+12,000	+36.44%

---

[a]Beginning in FY 2001, security investigations for non-federal personnel at Naval Reactors sites will be budgeted for in the Naval Reactors Development budget.

[b]Reflects Government-wide decrease of $336 thousand pursuant to FY 2000 Consolidated Appropriations Act rescission assigned to this program, and an increase of $4.913 million to allocate other program funds for security investigations of field non-federal employees.

[c]Does not reflect the use of at least $8.2 million in prior-year carryover. Reflects Omnibus rescission of $73 thousand assigned to this program.

Site Description

Operations Offices

The Security Investigations budget provides funding to the Personnel Security Offices to pay for background investigations conducted by the Federal Bureau of Investigation (FBI) and the Office of Personnel Management (OPM) for federal personnel and contractors. Background investigations are required for personnel who, in the performance of their official duties, require access to classified information or special nuclear material. The investigation is one of the tools used by DOE security personnel to determine if an individual will receive a security clearance.

Washington Headquarters

The Security Investigations budget provides funding for background investigations conducted by the FBI and OPM for Headquarter's Federal staff and contractors. This program also supports programs under Related Security Investigations Activities required to assure a viable personnel security function. This includes enhancements to the Electronic Transfer Program and DOE Integrated Safeguards and Security (DISS) personnel security databases to support additional functionality and security features.

Oak Ridge Institute of Science and Education

The Oak Ridge Institute for Science and Education (ORISE), located in Oak Ridge, Tennessee, provides DOE with technical support for implementation, training, operation, and quality assurance of the personnel security process, and a variety of research and analysis activities in support of personnel security functions. ORISE conducts these programs for DOE through a management and operating contract with Oak Ridge Associated Universities (ORAU).

Albuquerque Operations Office

In addition to providing funding to Albuquerque Operations Office for background investigations, it also receives funding for the costs to maintain the DOE Test Center/Accelerated Access Authorization Program (AAAP). Support through the Nonproliferation and National Security Institute (NNSI) is also provided to develop and distribute briefing materials as required by the refresher briefing provisions in DOE O 470.1, Chapter 4, "Safeguards and Security Awareness Program." Materials are posted on the NNSI web-site and made available to all DOE Federal and contractor sites required to provide refresher briefings to employees.

Security Investigations

Mission Supporting Goals and Objectives

The Security Investigations budget funds background investigations for DOE personnel and contractors who, in the performance of their official duties, require access authorizations for Restricted Data, National Security Information, or special nuclear material. Security Investigations are required in order to be in compliance with Section 145 of the Atomic Energy Act of 1954, as amended; Title 10, Code of Federal Regulations, Part 710; and Executive Order 12968, which mandate that access authorizations are required for access to classified information or special nuclear material. The Department primarily utilizes the services of the Office of Personnel Management (OPM) to conduct security investigations which serve as the basis for these access authorizations. FBI investigations are now required for individuals in positions that are of such a critical nature that any compromise could gravely impact U.S. national security. The cost of security investigations depends on the type and level of investigation needed.

Funding Schedule

	(dollars in thousands)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Federal Bureau of Investigation					
Initial Background Investigations	1,508	960	1,942	+982	+102.3%
Post-Initial Background Investigations (Reinvestigations)	450	1,969	7,945	+5,976	+303.5%
Federal User Charges	68	71	75	+4	+5.6%
Total, Federal Bureau of Investigation	2,026	3,000	9,962	+6,962	+232.1%
Office of Personnel Management					
Initial Background Investigations	13,817	8,711	13,978	+5,267	+60.5%
Reinvestigations	17,295	15,918	16,058	+140	+.0.9%
National Agency Checks	629	561	829	+268	+47.8%
Personnel Security Review	0	927	0	-927	-100.0%
Total, Office of Personnel Management	31,741	26,117	30,865	+4,748	+18.2%
Related Security Investigations Activities	3,810	3,810	4,100	+290	+7.6%
Subtotal, Security Investigations	37,577	32,927	44,927	+12,000	+36.4%
Less additional allocations from other program funds	-4,913	0	0	0	0.0%
Total, Security Investigations	32,664	32,927	44,927	+12,000	+36.4%

Case Projections

Category	FY 2000	FY 2001	FY 2002
Federal Bureau of Investigation (FBI)			
Initial Background Investigations	335	283	572
Post-Initial Background Investigations (Reinvestigations).	150	736	2,970
Subtotal, FBI Investigations	485	1,019	3,542
Office of Personnel Management (OPM)			
Initial Background Investigations	4,457	2,810	4,509
Reinvestigations	9,883	9,096	9,176
National Agency Checks	4,193	3,734	5,529
Subtotal, OPM Investigations	18,533	15,640	19,214
Total, Security Investigations	19,018	16,659	22,756

Detailed Program Justification

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Federal Bureau of Investigation (FBI)	**2,026**	**3,000**	**9,962**

As a result of the Defense Authorization Act for FY 2000 (S.1059, Section 3144), there has been a change in policy requiring personnel in positions that are of such a critical nature that any compromise could gravely impact U.S. national security to have background investigations conducted by the FBI. The FBI product is higher in cost than the OPM background investigation product (10% higher for initial investigations and 53% higher for reinvestigations). People in less sensitive positions will continue to have their investigations performed by the Office of Personnel Management. The funding level in FY 2002 will increase $6,962,000 mainly to accommodate the first full year requiring FBI investigation submissions. In FY 2001, the FBI is still in a transition period and accepting only limited DOE investigations.

# Initial Investigations	**1,508**	**960**	**1,942**

Conduct up to 572 initial background investigations. Plan to support 283 in FY 2001 (with an additional 132 cases being funded with prior-year carryover of approximately $448,000) and 335 in FY 2000.

# Post-Initial Background Investigations (Reinvestigations) . . .	**450**	**1,969**	**7,945**

Perform 2,970 periodic reinvestigations for FY 2002. Plan to support 736 in FY 2001 and 150 in FY 2000.

# Reimburse the FBI for fingerprint cards and name checks . .	**68**	**71**	**75**

Office of Personnel Management	**31,741**	**26,117**	**30,865**

Fund background investigations for DOE Federal personnel and contractors who do not require an FBI investigation, but require access authorizations for Restricted Data, National Security Information, or special nuclear material.

# Initial Investigations	**13,817**	**8,711**	**13,978**

Conduct 4,509 initial (Single Scope Background) investigations. Plan to support 2,810 cases in FY 2001(with an additional 2,380 cases that will be funded with prior-year carryover of approximately $7,378,000) and 4,457 cases in FY 2000. The $5,267,000 funding increase in FY 2002 does not take into consideration that $7,378,000 in prior-year funds and $8,711,000 in new budget authority (totaling $16,089,000) were used in FY 2001, and actually represents a decrease in funding of $2,111,000 in FY 2002.

# Reinvestigations	**17,295**	**15,918**	**16,058**

Perform 9,176 periodic reinvestigations (for Single Scope Background Investigations) which requires a slight funding increase over FY 2001 to cover 80 more cases. Project 9,096 cases in FY 2001 and 9,883 cases in FY 2000.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
# National Agency Checks (NAC's)	**629**	**561**	**829**

Conduct 5,529 NAC's. The "L" reinvestigations will resume with a substantial increase of 1,642 cases after 5 years of practically no activity. The reinvestigation interval for "L" access authorizations changed from 5 to 10 years in March 1997. Funding will increase to accommodate these cases. Plan to support 3,734 NAC's in FY 2001 and 4,193 cases in FY 2000.

# Personnel Security Review	**0**	**927**	**0**

In FY 2001, conducted a one-time personnel security review to evaluate security investigations performed by the FBI and OPM to compare the products to identify similarities and differences in the work completed by the two agencies. Funding has been redistributed to fund FBI security investigations in FY 2002.

Related Security Investigations Activities	**3,810**	**3,810**	**4,100**

Includes all costs incurred in implementing security investigations related programs and projects which may be developed in support of the Security Investigations Program.

# Continue operation and maintenance of the Electronic Transfer Program throughout DOE	**2,900**	**2,900**	**2,900**
# Continue to support the Accelerated Access Authorization Program (AAAP). A funding increase is necessary for expansion of the program to the east coast	**600**	**600**	**865**
# Provide support for miscellaneous costs involved in maintaining a viable personnel security program	**310**	**310**	**335**
Subtotal, Security Investigations	**37,577**	**32,927**	**44,927**
Less additional allocation from other program funds	**-4,913**	**0**	**0**
Total, Security Investigations	**32,664**	**32,927**	**44,927**

Explanation of Funding Changes
from FY 2001 to FY 2002

	FY 2002 vs. FY 2001 ($000)

 # Federal Bureau of Investigation (FBI)

- Funding level reflects an increase of $982,000 in initial background investigations due to the first full year requiring FBI investigation submissions . . . . **+982**

- Funding level reflects an increase of $5,976,000 in post-initial background investigations (reinvestigations) due to first full year requiring FBI investigation submissions . . . . **+5,976**

- Funding level reflects slight cost increase of $4,000 for reimbursing the FBI for fingerprint cards and name checks . . . . **+4**

Total, Federal Bureau of Investigation (FBI) . . . . **+6,962**

 # Office of Personnel Management (OPM)

- Initial background investigation estimates are based on specific site and contractor needs. The $5,267,000 increase does not take into consideration that $7,378,000 in prior-year funds and $8,711,000 in new budget authority (total $16,089,000) were used to fund initial investigations in FY 2001. In FY 2002, $13,978,000 is available for initial investigation which is actually a decrease of $2,111,000 over FY 2001. . . . . . . **+5,267**

- Reinvestigation activities show a slight increase with a major shift in funding now going to the FBI which is responsible for conducting investigations for individuals in critical positions. . . . . **+140**

- NAC's are increasing due to the "L" reinvestigation workload resuming with a substantial increase after 5 years of practically no activity. This is a result of the reinvestigation interval for "L" access authorization changing from 5 years to 10 years in March 1997. . . . . **+268**

- The FY 2001 review will be complete in regards to the OPM/FBI product study. Funding has been redistributed to fund FBI security investigations. . . . . **-927**

Total, Office of Personnel Management . . . . **+4,748**

	FY 2002 vs. FY 2001 ($000)

Related Security Investigations Activities

- A funding increase is necessary for the expected expansion of the AAAP to the east coast . . . .   +265
- A slight funding increase to cover miscellaneous costs involved in maintaining a viable personnel security program . . . .   +25

Total, Related Security Investigations Activities . . . .   +290

Total Funding Change, Security Investigations . . . .   +12,000

Corporate Management Information Program

Program Mission

A new decision unit has been created to provide funding for the Corporate Management Information Program (CMIP). CMIP is the Department's corporate investment initiative to replace outdated corporate information systems. CMIP provides a managed, disciplined, and cost-effective way to modernize DOE corporate business systems in a coordinated manner which uses new and emerging technologies and practices under the direction of CMIP review board with deliberative input of DOE line management. This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.

The Chief Information Officer conducts quarterly reviews of CMIP projects to assess adequacy of planning, review performance metrics, and determine if schedules are being met. Corrective action guidance is provided as necessary and discussed at subsequent reviews. Other guidance or direction, as appropriate, is provided to help ensure likelihood of each projects' successful development and ultimate full deployment. The CMIP Review Board conducts semiannual reviews of the entire program and provides overall direction.

Program Goal

To develop or install and maintain efficient and cost effective corporate management systems using new technology that will assist the Department of Energy in the accomplishment of its mission.

Program Objectives

The CMIP program was initiated by DOE in FY 1998 in recognition of the fact that corporate legacy systems that support administrative functions were nearing the end of their life cycles. An investment to replace and modernize severely outdated information technology (IT) systems would prove a much more efficient expenditure of scarce IT dollars than the continued enhancement, maintenance, and operation of the legacy systems. The CMIP design and implementation efforts fully support the mandates and principles of the Clinger-Cohen Act of 1996. The CMIP provides a cost-effective way to modernize and improve software applications, hardware, and infrastructure which support a wide range of Department-wide IT-based business systems. The outcome of the CMIP initiatives will be a secure, contemporary, interoperable, and cost-effective corporate information management system for the Department. Other anticipated benefits from CMIP strategic investments include faster response times on department-wide analyses and reports, improved decision-making based on better, more timely and accurate data and information, better ability to exercise fiduciary responsibilities for tax payer resources, and improved services to the public. A number of legislative and policy directives, listed below, created the need to establish an architecture-based, strategic information planning process.

\#   The Clinger-Cohen Act of 1996 requires the head of each Agency to establish an effective and efficient capital planning and investment control process for selecting, managing, and evaluating major IT investments, and prescribes minimum requirements for these processes. Clinger-Cohen also mandates that capital investment planning be based on an Agency IT architecture.

\#   The Office of Management and Budget (OMB) Circular A-130 establishes requirements for the development of IT architectures that agencies are required to meet.

\#   The OMB issued a policy statement in October 1996 citing Clinger-Cohen as the legal mandate for formulating effective long-term Agency strategies that provide multi-year plans for achieving mission goals. The statement also calls for the establishment of information architectures to guide investment decisions.

\#   The Government Performance and Results Act of 1993 requires Agencies to focus on program outcomes, establish measurable annual objectives that link to long-term goals, develop budgets based on planned performance, and report results.

\#   Congress has also enacted a number of changes to the original Freedom of Information Act concerning electronic records and Agency obligations.

The DOE *Information Architecture Volume IV, Vision* document, published in March 1998, marked the beginning implementation phase of the DOE Information Architecture (IA) Program. Developed over the past five years, the DOE IA Program defines the foundations, baseline, guidance, standards, and vision to serve as the basis for preparing an architecture-based, strategic IT plan. In early 1999, the Headquarters Information Architecture Project established a business case for performing a DOE IA project on corporate IT systems. Based on that business case, the Corporate Systems Information Architecture (CSIA) Project was initiated. The CSIA report was endorsed by the DOE Executive Committee for Information Management. The report includes a DOE Applications Architecture that identifies and defines a set of applications or automated capabilities DOE needs to conduct business that will support the shared data environment and provide the capability to store, share, and use data needed to conduct the Department's business efficiently. The CSIA identified thirty five applications needed and allows for technology infrastructure modernization projects to manage corporate data and support the DOE business functions.

Significant Accomplishments and Program Shifts

\#   This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.

Funding Profile

	(dollars in thousands)				
	FY 2000 Comparable Appropriation	FY 2001 Original Appropriation	FY 2001 Adjustments	FY 2001 Comparable Appropriation	FY 2002 Request
Corporate Management Information Program	0	0	0	0	20,000
Total, Corporate Management Information Program	0	0	0	0	20,000

Funding by Site

	(dollars in thousands)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Washington Headquarters	0	0	20,000	+20,000	+100.0%
Total, Corporate Management Information Program	0	0	20,000	+20,000	+100.0%

Corporate Management Information Program

Mission Supporting Goals and Objectives

The Corporate Management Information Program (CMIP) provides DOE with a managed, disciplined, and cost-effective way to modernize DOE corporate business systems, under the direction of the Department's Corporate Management Information Program Review Board, which is comprised of the Chief Information Office, Chief Financial Officer and the Director of the Office of Management and Administration, utilizing deliberative input from DOE Line Management. This is accomplished through the development/installation and maintenance of corporate management systems using new and emerging technologies.   This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account. The CMIP Review Board meets semiannually to allocate initiative project funding.

CMIP initiative projects in this budget include the following:

PHOENIX, formerly BMIS, which is a modern, responsive financial management system that is needed to aid managers to do more with less and focus on results. The existing financial management systems, which have been in use by DOE for almost 20 years, are not capable of responding rapidly to new demands for financial information from both internal and external customers. Due to the use of older technology and modifications over the years, these systems are difficult and expensive to maintain. In many instances, DOE Program Offices and field sites have developed their own auxiliary financial information systems to support their individual needs. This has resulted in the creation of duplicate systems, inconsistent information, and lack of interoperability. The need for a major change in DOE financial management practices is also driven by actions external to the Department, such as the Chief Financial Officer's Act of 1990, Government Performance and Results Act of 1993, Federal Financial Improvement Act of 1996, Clinger-Cohen Act of 1996, OMB Circular A-127, and Joint Financial Management Improvement Program.

Corporate Human Resource Information System (CHRIS) is the Department's official personnel system. CHRIS provides integrated human resource information functions for such areas as training, position management, and performance management. Personnel data from CHRIS is used to produce the payroll for employees and for financial, budget and resource reporting and planning. The day-to-day CHRIS operations and maintenance of the features and functions is funded through the Department's Working Capital Fund in FY 2002. CHRIS capabilities are being developed and implemented through CMIP to enable managers to track health and safety incidents, employee and labor relations cases, perform succession planning and other human resource functions now being performed either manually or by inefficient legacy systems.

Procurement Modernization is an effort to utilize computer information systems to improve and promote efficient use of resources in the Office of Procurement and Assistance Management.

\# **Information Architecture** that includes conceptual and process models, DOE-wide standards, principles, and a vision. The DOE IA Program defines the foundations, baseline, and guidance to serve as the basis for preparing an architecture-based, strategic IT plan. In early 1999, the Headquarters IA Project established a business case for preparing that plan. As a result, the DOE IA Project was initiated after endorsement by the DOE Executive Committee for Information Management. Phase One of the project defined a comprehensive high level IA Program that encompasses all components of DOE.

\# **Capital Planning and IT Investment** which is in response to the Clinger-Cohen Act of 1996 that directs Federal Agencies to use a comprehensive capital planning process for selecting, managing, and assessing IT investments. To this end, DOE established the DOE IT Capital Planning and Investment Process in 1998, representing significant progress toward enhanced decision-making. The evolving process provides an analytical framework for linking IT investment decisions to strategic objectives, mission achievement, and business plans. The Departmental process applies primarily to crosscutting corporate administrative and infrastructure initiatives. Program and Field Offices are responsible for similar processes to link their IT investments to mission priorities.

\# **Strategic Information Management (SIM)** program which ensures strategic alignment of major IT investments with DOE business goals and objectives to maximize improvements in mission performance. SIM techniques identify organizational business needs that can be met effectively and efficiently through IT investments, justifying each dollar against business objectives and processes. The SIM process is used to study cross-functional segments of an organization, identifying relationships between business processes and their alignment with IT investments. By achieving strategic alignment among key process elements, significant cost savings and business improvement opportunities are realized.

\# **Corporate Systems Information Architecture (CSIA) Initiatives** The DOE Information Architecture (IA) Program CSIA Project study began a comprehensive review of existing and required corporate systems to develop a proposed migration plan for corporate system modules. This project study included, but extended beyond, the traditional business systems such as personnel, payroll, time and attendance, labor distribution, financial management, and procurement. Project findings pointed to potential significant long-term savings in IT investments if systems support common missions of the Department's program offices. Significant benefits are expected in such areas as strategic and program planning, core data management, physical asset management, communication and outreach, and project management when legacy systems are replaced or modernized under a corporate systems approach. The final report included a CSIA DOE Applications Architecture with recommendations for potential expansion of CMIP to encompass non-administrative critical program mission support systems.

\# **CSIA Technology Infrastructure Modernization** The DOE Information Architecture (IA) Program CSIA Project study identified thirty five applications needed to manage corporate data and support the DOE business functions. The FY 2002 Budget Request allows for four technology infrastructure modernization projects which are: DOE Headquarters Network Switching Infrastructure Upgrade and

IT Systems Dispersed Client Server Management Framework (Tivoli); Migration of DOE Headquarters Server Operating System from Novell Netware to Windows NT; Develop and Implement a Comprehensive Data Backup, Restoration and Offsite Disaster Recovery Service for DOE Headquarters Customers; and DOE Headquarters Microsoft Exchange Infrastructure Upgrade.

Funding Schedule

	(dollars in thousands)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Corporate Management Information Program	0	0	20,000	+20,000	+100.0%
Total, Corporate Management Information Program	0	0	20,000	+20,000	+100.0%

Detailed Program Justification

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Corporate Management Information Program……………...	**0**	**0**	**20,000**

PHOENIX

The FY 2002 Budget Request allows the Phoenix (formerly BMIS-FM) project design and implementation activities to continue.

- Complete the design phase for the core financial system.

- Complete the configuration phase of the core financial system.

- Complete training and other readiness preparation activities for a minimum of one service center and its related satellite offices.

- Complete critical software system interfaces.

- Complete Independent Validation and Verification (IV&V) testing.

- Complete installation and cut-over to production for a minimum of one service center and its related satellites.

- Complete the software and work process gap analysis of Budget Formulation requirements.

Corporate Human Resource Information System

FY 2002 Budget Request allows CHRIS development activities to continue.

- Identify one or two HR functions as implementation priorities based on Department-wide needs and the degree of Federalization of the software at the time of their decision.

- Complete fit/gap analyses of the functions as delivered in the PeopleSoft Federal product software and the Department's business processes.

- Design, develop, test and implement functions approved in the previous year.

- Maintain CHRIS as a state-of-the-art system by appropriately planning for and implementing PeopleSoft Federal release upgrades to assure that the Department takes advantage of planned technology and functional improvements in the commercial-off-the-shelf product.

- Implement at least one re-engineered human resource business process each fiscal year utilizing CHRIS or the CHRIS web-site.

- Reduce the number of legacy and local HR systems.

Procurement Modernization

FY 2002 Budget Request allows Procurement Modernization approved Strategic Information Management (SIM) Business Case development activities to begin.

Information Architecture

FY 2002 Budget Request allows IA activities to continue, but at a slower pace, and some planned activities may slip to FY 2003.

- Continue detailed analysis, definition and modeling of the DOE technology architecture to ensure alignment and integration with the Security Architecture and the Corporate IT Infrastructure Initiative.

- Implement an Information Architecture policy and assessment capability to evaluate all Corporate Capital IT investments and to ensure that the DOE IA is updated and maintained.

- Develop and begin implementation of a management matrix to monitor and measure interoperability of Corporate Systems and technology capability deployments.

- As Program and site architectures are completed, expand the DOE Information Architecture (Business Model, Data and Applications Architectures) to cover and include the Programmatic Components (Missions Functions) of the Department.

- Complete formalized architectural assessment documentation for all current Corporate Capital IT Investments and update them, as appropriate, during the investment life cycles.

- The Corporate IA Business Model, Data and Applications Architectures are expanded and updated.

- The Corporate Technology Architecture documentation is completed and is aligned and integrated with the Security Architecture and the Corporate IT Infrastructure Initiative.

- The Interoperability Matrix is implemented and is tracking implementations of Corporate IT Investments (Systems and Capabilities) across the DOE Federal sites.

Capital Planning and IT Investment

FY 2002 Budget Request allows Capital Planning and IT Investment activities to continue, but at a slower pace, and some planned activities may slip to FY 2003.

- Efforts to ensure DOE Program offices apply capital planning principles to their IT investments will continue.

- Maintain an effective Capital Planning and IT Investment Control Process.

- DOE Program Offices apply the principles of the DOE Guide to IT Capital Planning and Investment to their IT investment processes.

- Corporate IT Investment Board; Executive Committee for Information Management, and CIO Executive Council make Capital Planning decisions throughout the year.

- Improve Corporate Management Information Program through use of an enhanced Corporate IT Management Process.

- Semiannual CMIP Review Board program reviews conducted.

- CIO Quarterly Program Reviews will continue to be conducted.

- CMIP Annual Reports will be provided to Congress.

Strategic Information Management

FY 2002 Budget Request allows SIM activities to continue at a slower pace than planned. SIM has a structured process to evaluate business requirements, determine systems needed and identify existing system shortfalls. The SIM process produces business case analyses leading to recommendations for new or enhanced corporate information technology investments.

CSIA Initiatives

The CSIA Applications Architecture identifies and defines a set of applications or automated capabilities DOE needs to conduct business that will support the shared data environment and provide the capability to store, share, and use data needed to conduct the Department's business efficiently. Currently, the CSIA has identified thirty five applications needed to manage corporate data and support the DOE business functions.

FY 2002 Budget Request allows development activities to begin on the following three CSIA initiatives after SIM Business Cases have been approved:

1. Departmental Element Information Repository - The repository will allow the Department to maintain a uniform and current file of basic data on all of DOE to support other automated systems across the enterprise. The repository will also assist in communication both within DOE and with its customers. Potential benefits of the repository include: accurate information, consistent information about all DOE organizational units across the complex, current information, facilitate response to ad hoc inquiries, available across DOE and to customers.

2. Information Structure Repository - The repository will allow the Department to provide a comprehensive, official, and current file of the name and code identification of important categories of information such as B&R codes, contractor identification, and employee categories. Potential benefits of the Information Structure Repository include: codes and values are centrally managed, with clear indications of who is responsible for maintaining the data, permitting ease and consistency of updates and corrections; the same codes and values are used for all systems, saving time and money in avoiding duplicate maintenance, data entry, etc; cross-cutting data aggregation is enabled in systems, as codes and queries are guaranteed to be the same for all systems.

3. Organization Information Repository - The repository will allow the Department to provide an easily accessible, accurate, complete and current source of basic information about non-governmental organizations with whom DOE does business such as contractors, grantees, public interest groups and suppliers. Potential benefits of the Organization Information Repository include: accurate information; consistent information about all organizations with whom DOE conducts business; current information; provides response to ad hoc inquiries; available across DOE.

CSIA Technology Infrastructure Modernization

The CSIA identified thirty five applications needed to manage corporate data and support the DOE business functions. The FY 2002 Budget Request allows for the following four technology infrastructure modernization projects:

1. DOE Headquarters Network Switching Infrastructure Upgrade and IT Systems Dispersed Client Server Management Framework (Tivoli) - The DOE Headquarters network switching infrastructure requires an upgrade in several organizational areas for achieving greater grade of service in distribution of information and data to the desktop and enhancing the use of multi-media services. Architectural framework and associated tools, processes and procedures are needed for ensuring 99%+ availability of IT network services to the end users through proactive management. Expanding the employment of Tivoli (a proprietary COTS product) system management agents throughout DOE Headquarters will allow DOE IT systems management personnel to analyze any data from many different perspectives, compare current activities to historical records, spot trends for capacity planning and resource forecasting, isolate trouble areas, evaluate resource allocations and project future requirements and associated fiscal assets.

2. Migration of DOE Headquarters Server Operating System from Novell Netware to Windows NT
Currently the DOE HQ network supported by the Office of the CIO is running on two different network operating systems, Novell Netware and Windows NT. The mixed environment degrades network efficiency, security, administration and effective user interface. Novell plans to stop supporting E-Mail software (SFT III) on December 31, 2001; therefore, it is imperative to convert the operating systems to Windows NT to allow DOE HQ to continue using the HQ E-Mail system to communicate beginning in calendar year 2002. Standardizing the operating system infrastructure also minimizes customer confusion and support personnel costs required to support a mixed Novell NetWare/Windows NT operating platform, two protocols, separate passwords and separate teams for administration.

3. Develop and Implement A Comprehensive Data Backup, Restoration and Offsite Disaster Recovery Service for DOE Headquarters Customers - Currently at DOE Headquarters there are a variety of solutions in place, or no solution at all, for backup and recovery. This means that every system, including desktop systems, must deal with their backup and recovery needs and manage these needs separately. This approach is wasteful of both resources and people. Providing a comprehensive backup and recovery business line with workload distributed between Forrestal and Germantown to mitigate power outages or other problems at either location, would relieve customers of this concern and allow them to concentrate on their mission.

4. DOE Headquarters Microsoft Exchange Infrastructure Upgrade - The DOE's Office of the CIO developed and maintains an Infrastructure that allows all Headquarters' Program Offices to communicate effectively using Electronic Mail. Recently, Microsoft Corporation released a new version of their E-Mail system called Exchange 2000. This new E-Mail system relies upon the recently released operating system known as Windows 2000. At issue is the fact that Exchange 2000 relies upon the Windows 2000 Active Directory in order to function. To maintain a fully functional E-Mail environment at DOE Headquarters, there must exist a single Active Directory Forest. Should DOE Headquarters' fail to introduce a single Active Directory Forest current E-Mail Exchange interoperability will cease to exist.

Explanation of Funding Changes
from FY 2001 to FY 2002

FY 2002 vs. FY 2001 ($000)

- **This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.**   +20,000

Security and Emergency Operations Program Direction

Mission Supporting Goals and Objectives

The Program Direction program supports and provides for Federal personnel and associated funding required to provide overall direction of activities carried out in the Office of Security and Emergency Operations (SO) under the following programs: Offices of Chief Information Officer, Security Affairs, Critical Infrastructure Protection, and Resource Management. SO also provides program-specific staffing resources at the Chicago Operations Offices directly involved in executing SO's programs. These activities are carried out in a cost effective and efficient manner.

In FY 2002, the Program Direction associated with the Emergency Management and Emergency Response programs will be transferred to the Weapons Activities Appropriation for the National Nuclear Security Administration (NNSA). In addition, the Program Direction associated with the HAZMAT Spill Test Facility at the Nevada Test Site has been transferred to the Office of Defense Nuclear Nonproliferation's Research and Development decision unit in the Other Nuclear Activities Appropriation for the NNSA.

Program Goals

\#   Fund Salaries and Benefits, Travel, Support Services, and Other Related Expenses, the latter including the Working Capital Fund, associated with the overall management, direction, and administration of the following programs: Nuclear Safeguards and Security; Classification/ Declassification; Plutonium, Uranium, and Special Material Inventory; Foreign Visits and Assignments; Chief Information Officer; Critical Infrastructure Protection; and Resource Management.

Program Objectives

\#   To provide Salaries and Benefits for SO Federal employees, including overtime, awards, lump-sum leave payments, transit subsidies, contributions to employee benefits, and associated cost-of-living increases.

\#   To provide Travel funds that are required to carry out SO's mission while away from official duty stations. Ensure per diem allowances as well as local travel are in accordance with Federal Travel Regulations. Travel is an essential part of staff duties in order to conduct hands-on operations both domestically and internationally, participate in highly technical agency and interagency committees, and to ensure appropriate Government representation in policy meetings.

\#   To provide Support Services contracts to support Federal Staff at Headquarters and in the field. These contracts provide technical, analytical, administrative, and operational support for the following multiple program areas.

- Provide Support Services contract funding for technical and analytical support to the initiatives of the Chief Information Officer based on the Clinger-Cohen Act, operational and infrastructure requirements.

- Provide technical, analytical, administrative, and operational support in multiple program areas of safeguards and security, critical infrastructure, and resource management. The daily operation and associated technical direction of the contracts remain with Federal program managers in each organization.

\# To provide funding for Other Related Expenses that includes the Working Capital Fund. Other Related Expenses support the administrative costs of maintaining Federal Staff, such as information technology expenses, training, and other miscellaneous services. The Working Capital Fund includes centrally provided goods and services at Headquarters, such as space, utilities, general printing, graphics, copying, supplies, postage, telephones, supplies, and rent.

Funding Schedule

	(dollars in thousands, whole FTEs)				
	FY 2000	FY 2001	FY 2002	$ Change	% Change
Chicago					
Salaries and Benefits	4,241	4,408	4,611	+203	+4.6%
Travel	162	142	142	0	0.0%
Support Services	180	170	170	0	0.0%
Other Related Expenses	1,320	1,305	2,017[a]	+712	+54.6%
Total, Chicago	5,903	6,025	6,940	+915	+15.2%
Full Time Equivalents	56	58	58	0	0.0%
Headquarters					
Salaries and Benefits	28,497	33,109[b]	34,723	+1,614	+4.9%
Travel	1,503	1,890	1,696	-194	-10.3%
Support Services	32,782[c]	21,688	20,885	-803	-3.7%
Other Related Expenses					
Other - Desktop	0	0	2,001	+2,001	+100.0%
Other	14,234	17,710	16,890	-820	-4.6%
Total, Other Related Expenses	14,234	17,710	18,891	+1,181	+6.7%
Total, Headquarters	77,016	74,397	76,195	+1,798	+2.4%
Full Time Equivalents	278	329	329	0	0.0%
Total Security and Emergency Operations					
Salaries and Benefits	32,738	37,517	39,334	+1,817	+4.8%
Travel	1,665	2,032	1,838	-194	-9.5%
Support Services	32,962	21,858	21,055	-803	-3.7%
Other Related Expenses					
Other - Desktop	0	0	2,001	+2,001	+100.0%
Other	15,554	19,015	18,907	-108	-0.6%
Total, Other Related Expenses	15,554	19,015	20,908	+1,893	+10.0%
Subtotal, Program Direction	82,919	80,422	83,135	+2,713	+3.4%
Less Security Charge for Reimbursable Work	0	0	-712	-712	N/A
Total, Program Direction	82,919	80,422	82,423	+2,001	+2.5%
Full Time Equivalents	334	387	387	0	0.0%

[a]Includes $712,000 for reimbursable work adjustments for safeguards and security.

[b]FY 2000 unobligated funding of $1,425,734 remaining from the $3,000,000 Supplemental Appropriation was used for FY 2001 payroll requirements.

[c]Includes $12,000,000 received in the FY 2000 Supplemental Appropriation for the CIO to address unclassified cyber security systems.

Detailed Program Justification

	FY 2000	FY 2001	FY 2002
Salaries and Benefits	**32,738**	**37,517**	**39,334**

SO staff serves as the Headquarters operational element for activities such as safeguards and security; critical infrastructure protection; enhanced foreign visits and assignments; plutonium, uranium, and special material inventory; declassification and classification operations; and provides staff for the Office of the Director and Resource Management. Increases fund cost-of-living adjustments, promotions, within grade increases, lump-sum payments, and overtime. Performance will be measured by an adequate Federal staff to successfully perform SO's programmatic goals and objectives.

Staff develops Department-wide policy and plans for National Security Programs such as Safeguards and Security and the Nuclear and National Security Information. SO is directly responsible for management of the New Brunswick National Laboratory in Argonne, Illinois and the Nonproliferation and National Security Institute in Albuquerque, New Mexico.

Staff within the Critical Infrastructure Protection program carry out the National mandates of the Critical Infrastructure Protection directive and Presidential decision Directive 63 regarding critical infrastructure protection. These mandates obligate DOE to partner with the private sector in ensuring the viability of the energy sector infrastructures nationwide.

Staff of the Chief Information Officer functions are to develop and issue policy, procedures, and guidance on the management of information and information technology (IT) across the Department and Government-wide through the Federal Chief Information Officer Council; establish, implement, and maintain a comprehensive cyber/computer security program to protect the Department's classified and unclassified information and information technology assets; manage the Corporate Management Information Program jointly with the Office of Chief Financial Officer and the Office of Management and Administration; produce Departmental IT reports required by the White House and Congress; promote and facilitate the evolution and growth of Departmental electronic Government products emphasizing web-based capabilities as efficient tools for public service; and provide improved Headquarters desktop services including a unified and effective help desk, timely response and support of DOE missions via a reliable and cost effective DOE corporate network, local and long distance telephone services, pagers and cellular telephones, and video conference support.

Performance is measured for the Chief Information Officer's function by how well the Department ensures economical and effective management of information resources to support DOE missions and objectives; makes effective use of commercial applications and solutions for DOE's enterprise-wide IT infrastructure; links IT investments to DOE strategic goals and the needs of business operations; minimizes the number of redundant and duplicative systems; and improves enterprise-wide data sharing.

\# Staff in the Foreign Visits and Assignments function develop and promulgate policy and guidance and perform in-depth program oversight for all foreign visits and assignments to DOE and DOE contractor facilities nation-wide (including DOE Headquarters and the National Laboratories) and for foreign national contact with DOE and DOE programmatic and technical persons. The Office acts as a central accounting center to track and analyze the details of all foreign visits and assignments to all DOE and DOE contractor facilities to ensure that these are conducted in a secure manner.

\# Staff in the Office of Plutonium, Uranium, and Special Materials Inventory are responsible for the accurate and reliable tracking of strategic nuclear materials and analysis of nuclear material inventory data for purposes of identifying accountability-related issues.

	FY 2000	FY 2001	FY 2002
Travel	1,665	2,032	1,838

\# Includes domestic and foreign trips necessary to conduct security and the Chief Information Officer's activities. Domestic travel includes national security assistance and interface with field offices, laboratories and local governments. Additionally provides travel for the Executive Protection Security personnel. Decreases are a result of reduced training requirements, therefore, requiring less travel funding.

\# Performance is measured by ensuring travel funding is adequate to allow the appropriate amount of onsite supervision by Federal staff of SO activities throughout the DOE complex.

	FY 2000	FY 2001	FY 2002
Support Services	32,962	21,858	21,055

\# Provides an invaluable resource of highly specialized and analytical expertise required to meet critical security operations issues. Performance will be measured by SO obtaining an adequate level of specialized contractors to ensure the successful performance of SO's programmatic goals and objectives.

\# Provides technical and analytical expertise as well as management support essential to carry out the safeguards and security program. Support Services decrease slightly because of reductions in contracting activities as vacancies for permanent Federal staff positions are minimized.

\# Provides a proactive program that interfaces with the private sector, other Government agencies, and the Executive Branch in establishing mutual support arrangements in the furtherance of the DOE Critical Infrastructure Protection Program.

\# Provides technical and analytical support to initiatives of the Chief Information Officer based on the Clinger-Cohen Act, operational and infrastructure requirements. Additionally, funding in the amount of $12,000,000 was received in a FY 2000 Supplemental appropriation to address unclassified cyber security systems and security needs in the corporate management information systems to be managed and executed by the Chief Information Officer.

	(dollars in thousands)		
	FY 2000	FY 2001	FY 2002
Other Related Expenses - Desktop	**0**	**0**	**2,001**

Supports the desktop information technology requirements provided through the Chief Information Officer for Local Area Network connectivity, e-mail services, hardware and software acquisitions, and networking upgrades. This funding has been transferred to SO in FY 2002 and was previously funded in the Departmental Administration account.

	FY 2000	FY 2001	FY 2002
Other Related Expenses	**15,554**	**19,015**	**18,907**[a/]

Includes Headquarters space, utilities, general printing, graphics, copying, supplies, telephones, general automation support, payroll processing, postage, and other miscellaneous expenses associated with office operations. Other Related Expenses slightly decrease due to one-time expenses in FY 2001 for computer equipment and Local Area Network upgrades, and lower training requirements due to the leveling off of new hires.

Similar support is provided to the Federally staffed New Brunswick Laboratory.

SO funding for the Working Capital Fund is included in this subprogram and remains level with requirements in FY 2001. The performance measure for the support of the activities funded under the Working Capital Fund is to control costs associated with these activities where possible and to adequately fund them through the budget process. SO regularly monitors all expenditures in the Working Capital Fund and has reduced, to the extent possible, utilization of services provided through this fund. Further per capita reductions, in keeping with good business practices, in utilization of the services provided through this fund is a performance measure SO sets for itself in this account.

	FY 2000	FY 2001	FY 2002
Subtotal, Program Direction	**82,919**	**80,422**	**83,135**
Less Security Charge for Reimbursable Work	**0**	**0**	**-712**
Total, Program Direction	**82,919**	**80,422**	**82,423**

---

[a]Includes $712,000 for reimbursable work adjustments for safeguards and security.

Explanation of Funding Changes from FY 2001 to FY 2002

	FY 2002 vs. FY 2001 ($000)

 # Salaries and Benefits

Salaries and Benefits increase to fund cost-of-living increases, promotions, within grade increases, lump sum payments, and overtime.   **+1,817**

 # Travel

Travel decreases slightly to allow sufficient increases in salaries and benefits in a level budget between FY 2001 and FY 2002 for required cost of living increases. Additionally the training budget has decreased, therefore, not requiring as much travel funding.   **-194**

 # Support Services

Support Services decrease slightly because of reductions in contracting activities as vacancies for permanent Federal staff positions are minimized.   **-803**

 # Other Related Expenses

  ! Increase due to funds being transferred in FY 2002 to SO from the Departmental Administration account to fund desktop information technology requirements provided through the Chief Information Officer for Local Area Network connectivity, e-mail services, hardware and software acquisitions, and networking upgrades.   **+2,001**

  ! Other Related Expenses decrease due to one-time expenses in FY 2001 for computer equipment and Local Area Network upgrades.   **-567**

  ! Training requirements decrease due to the leveling off of new hires and one-time training requirements being expended in FY 2001.   **-253**

Security Charge for Reimbursable Work	+712
Subtotal Funding Change, Program Direction	+2,713
Less Security Charge for Reimbursable Work	-712
Total Funding Change, Program Direction	+2,001

Support Services

(dollars in thousands)

	FY 2000	FY 2001	FY 2002 Request	$ Change	% Change
Technical Support Services					
System Review & Reliability Analysis . .	141	458	345	-113	-24.7%
Test and Evaluation Studies	141	458	345	-113	-24.7%
Technical Operation Reviews	6,912	7,227	7,087	-140	-1.9%
Critical Infrastructure Protection Analysis and Reporting	392	421	421	0	0.0%
Total Technical Support Services	7,586	8,564	8,198	-366	-4.3%
Management Support Services					
Management Studies	5,131	1,576	1,382	-194	-12.3%
Training and Education	246	113	113	0	0.0%
ADP Support	16,496	8,363	8,363	0	0.0%
Administrative Support Services	3,503	3,242	2,999	-243	-7.5%
Total, Management Support Services . . .	25,376[a]	13,294	12,857	-437	-3.3%
Total Support Services	32,962	21,858	21,055	-803	-3.7%

Other Related Expenses

(dollars in thousands)

	FY 2000	FY 2001	FY 2002 Request	$ Change	% Change
Other - Desktop	0	0	2,001	+2,001	+100.0%
Working Capital Fund	7,802	8,452	8,452	0	0.0%
Training	292	896	643	-253	-28.2%
Other[b]	7,460	9,667	9,812[c]	+145	+1.5%
Total, Other Related Expenses	15,554	19,015	20,908	+1,893	+10.0%

---

[a]Includes $12,000,000 received in the FY 2000 Supplemental Appropriation for the CIO to address unclassified cyber security systems.

[b]Other includes equipment and the operation and maintenance of equipment.

[c]Includes $712,000 for reimbursable work adjustments for safeguards and security